



המלצות אבטחת מידע ופרטיות

✂ **מלחמת חרבות ברזל** ✂

תורמים לכתיבת המסמך:

• קובי ויזר - מומחה סייבר
• מיטל דהרי - מומחית אבטחת מידע
• ניר יהונתן פסי CISO
• איתמר שלו - מומחה סייבר

• יובל שגב - יו"ר פורום הסייבר באיגוד הדירקטורים
• דני אברמוביץ - מנכ"ל טייטנס סקויריטי ונשיא
של הצ'אפטר הישראלי באיגוד העולמי לאבטחת מידע (ISSA)
• יגאל אקרמן ואור ישראל לוי - יועצי אבטחת מידע מחברת טייטנס סקויריטי

להערות או המלצות לשיפור המסמך, ניתן לשלוח כל תגובה לכתובת: yuvalsegev80@gmail.com

תוכן עניינים:

3 חלק 1 – כללי
4 הנחות עבודה:
5 סיכונים ותרחישים לדוגמא:
6 חלק 2 – הנחיות וכללי זהירות בנושא אבטחת מידע והגנת הפרטיות
7 הנחיות אבטחת מידע והגנת הפרטיות כלליות
9 כללי זהירות במדיה חברתית
11 כללי זהירות למשתמשים באפליקציית WhatsApp
13 כללי זהירות למשפחות השכולות, החטופים והנעדרים
14 כללי זהירות לארגונים שמנהלים יוזמות התנדבות ותרומות
15 כללי זהירות והמלצות לשימוש באפליקציות של מסמכים שיתופיים
16 כללי זהירות להורים
17 כללי זהירות לכוחות הביטחון
18 נספח א' - מילון מונחים
20 נספח ב' – כיצד ניתן לזהות האם מדובר בלינק (קישור לאתר אינטרנט) זדוני?

חלק 1 – כללי

מבוא:

בעת מלחמה, ההגנה על המידע והפרטיות של האזרחים, ושמירה על בטיחות כוחות הביטחון, הופכת לקריטית עוד יותר. אנחנו נמצאים במלחמה עם אויב שלא יודע שובע, והמעשים בשבוע האחרון הוכיחו לנו את אכזריותו. בצער רב, לידיו נפלו מכשירי טלפון רבים של חיילינו ואזרחנו היקרים, וכעת לאויב יש גישה למכשירים אלו ולמידע שאגור בהם.

בנוסף, ברחבי העולם יש אנשים שפרו-פאלסטינאים, ומטרתם להפיץ פייק ניוז ברשתות החברתיות ולהוציא אותנו לא טוב מול העולם.

שמירה על המידע והפרטיות חשובה למניע נזקים פוטנציאליים לאזרחים, לכוחות הביטחון ולבטחון הלאומי. מידע רגיש שנפל או יפול בידי האויב יכול לשמש לצרכים צבאיים נוספים או לגרום תעמולות בעולם.

מסמך זה נכתב על ידי קבוצת עבודה מהשוק הפרטי, במטרה להנגיש מידע רלוונטי לכל האזרחים.

לציבור הרחב הישראלי, הציאפטר הישראלי של האיגוד העולמי לאבטחת מידע (ISSA), בשיתוף עם מומחי אבטחת מידע בתעשייה הישראלית בהובלת **יובל שגב** עמלו והכינו מספר מדריכים וסרטונים במטרה להגביר את המודעות של הציבור לאיומי וסיכוני סייבר, ולהקטין את הסיכון ליפול קורבנות למתקפות סייבר שונות.

ניתן לצפות בסרטונים באתר של האיגוד, בכתובת:

[/מוקד-מידע/issa.org.il](https://issa.org.il)

בנוסף, תודה רבה לכל מי שתרום ליצירת המסמכים והמדריכים. להוספת תגובות והמלצות למסמך, ניתן לפנות ל**יובל שגב**, במייל yuvalsegev80@gmail.com.

הנחות עבודה:

- לאויב יש אינטרס לייצר לחץ פסיכולוגי ותודעתי. פעולות הפחדה, סחיטה, הפצה של פייקניוז, עשויות להוות חלק מהמערכה.
- טלפונים סלולריים של כמה מאלו שאינם בין החיים או נפלו בשבי נלקחו, והאויב מתחבר לקבוצות הווטסאפ שלהם, לפרופיל הלינקדין ולרשתות חברתיות שלהם. [דוגמא לכך](#), ראינו כאשר אחד המחבלים רצח קשישה, והעלה סרטון לפרופיל הפייסבוק של הנרצחת. אנו לרוב נוטים לסמוך על הודעות שמתקבלות ממקור איתו יש לנו היכרות אישית. בימים אלו, יש לבחון בזהירות הנחת מוצא זו, עד לחזרה לשגרה.
- בעת מצבי קיצון (כגון מלחמה), אנו נוטים לרוב לסמוך על אנשים אחרים וגופים שמפרסמים ומציעים תמיכה, תרומות, וסיוע לנזקקים. בימים אלו, יש לבחון בזהירות הנחת מוצא זו, ולהיות חשדנים יותר.
- רוב ההודעות ברשתות החברתיות הינן פייק. הפצתן אינה מסייעת, ואף גורמת לנזק.

מומלץ לפעול בהתאם להמלצות פיקוד העורף בנושא:

- ✓ האם המידע הגיע ממקור מהימן?
- ✓ האם שיתופו עלול לפגוע במישהו?
- ✓ האם הפצת המידע יכולה לסייע איכשהו?

סיכונים ותרשישים לדוגמא:

סחיטה – מצב שבו מישהו זדוני (במקרה הזה האויב) איים על אדם אחר (במקרה הזה, בני המשפחה או חברים) אם אותו אדם לא יעשה מה שמבקשים ממנו.

- **תרשיש אפשרי:** האויב רואה ברשתות החברתיות את התמונה של האדם שנעדר, מתקשר למשפחה ומנסה לסחוט אותה בתמורה [לקבלת מידע](#).

זליגת מידע רגיש – הגעתו של מידע רגיש (כגון נתוני מיקום, טלפונים, כתובות, וכדומה), בידי אדם זר (במקרה הזה האויב), שינצל אותו לביצוע פעילויות זדוניות.

- **תרשיש אפשרי:** האויב ינסה להתחבר לקבוצות ווטסאפ במטרה לשאוב משם מאגרי מידע רגישים שנבנים מתוך מטרה טובה ([דוגמא למאגר](#) עם מידע רגיש וניהול הרשאות לא מיטבי) או יקים קבוצה כזו, אשר בהתחלה תפעל בצורה לגיטימית ([דוגמא לקבוצה שמציעה לאנשים שמחפשים טרמפ דרומה](#)).
- **תרשיש אפשרי:** האויב יישאב מידע רגיש ויקבל תמונת מצב מתוך פרסומים וריכוזי נתונים שנבנים בצורה "פתוחה" ללא בקרה (ראו [דוגמא מאגר איתור נעדרים](#)), בו ניתן לשאוב את כל המאגר בקלות באמצעות הקשת כל ה א-ב).
- **תרשיש אפשרי:** האויב יקים אתר אשר מתיימר לסייע (נניח, איתור נעדרים) במטרה לקבל מידע רגיש כגון מיקום, תפקיד בצבא וכו' מקהל יעד מטורגט. זה יאפשר לו לאסוף מידע רגיש אודות כוחות הביטחון.
- **תרשיש אפשרי:** האויב ינסה להוציא מידע ממכשירים סלולריים ו/או לבצע פעולות בשמם של החטופים/נרצחים (העברה כספית, הוצאת מידע רגיש, יצירת קשר עם קרובים או קולגות וכו').

התחזות והפחדה – מצב שבו גורם זר (במקרה הזה האויב) יתחזה לאדם אחר (במקרה הזה לאחד החטופים או נעדרים), וינסה לבצע פעולות בשמו (כגון ביצוע עסקאות מקוונות), או פעולות הסתה והפחדה (לפרסם בשמו תמונות וסרטונים בקבוצות דיון שונות וברשתות החברתיות).

- **תרשיש אפשרי:** האויב ייכנס דרך מכשירי טלפון של אנשים שנחטפו לרשתות חברתיות וישלח הודעות בשמם, או יכריח אותם להקליט הודעות (פייק ניוז) במטרה לייצר בהלה ולהעביר מסרים וכו'.

חלק 2 – הנחיות וכללי זהירות בנושא אבטחת מידע והגנת הפרטיות

כללי

המסמך מרכז בתוכו מגוון רחב של טיפים ועיצות, במטרה לסייע ולהגביר את המודעות של כלל הציבור בישראל לסיכונים פוטנציאליים בעידן הדיגיטלי, ובעת המלחמה.

לנחיותכם, ריכזנו לכם לפי נושאים וקהל יעד, מספר טיפים והמלצות שניתן ליישם במטרה למנוע ולהקטין את הסיכון לפגיעה בפרטיות, הפצת פייק ניוז, בהלה, או מעילות והונאות.

הנחיות אבטחת מידע והגנת הפרטיות כלליות



גם בעת מלחמה, וגם בשגרה, מומלץ לאמץ את הכללים הבאים לשמירה על אבטחת מידע אישי, והגנת הפרטיות שלכם:

1. **חשבונות משתמשים** – חשבון משתמש מורכב לרוב משני אמצעי זיהוי ואימות. אמצעי הזיהוי הראשון זה פרט מזהה שלכם (למשל שם, מספר ת.ז., כתובת דואר אלקטרוני, וכדומה), והפרט אימות זה משהו שרק אתם יודעים (כגון סיסמה). כולנו משתמשים בחשבונות משתמשים לצורך גישה לאפליקציות ושירותים מקוונים שונים (כגון בנקים, חברות הביטוח, קופת חולים, חברות תעופה, תיבת דואר אלקטרוני אישית, ועוד). מרבית האנשים נוהגים להשתמש באותו חשבון לגישה לכל השירותים אותם הוא צורך בחיי היום-יום, דבר שמגדיל את הסיכויים לגניבת זהויות והשתלטות על החשבונות שלכם. מומלץ לייצר 2 חשבונות משתמשים:
 - **חשבון אחד פרטי** – שימש אתכם רק לצורך גישה לשירותים הפרטיים החשובים שלכם (כגון שירותים פיננסיים, רפואיים, טיסות וכדומה).
 - **חשבון שני כללי יותר** – שימש אתכם להרשמה לאתרים שונים (כגון התנדבות, וכדומה).
2. **בדיקת חשבונות** – מדי פעם (יומי או שבועי), מומלץ לבדוק את החשבונות האישיים שלכם (חשבון הבנק, חברת הביטוח, רפואי, רשתות חברתיות, דוא"ל וכדומה), לוודא שאכן אתם מצליחים להיכנס לחשבונות שלכם, ושאינן תנועות חריגות.
3. **סיסמאות:** הסיסמאות מספקות הגנה מפני גישה לא מורשית למידע אישי שלכם, כגון חשבונות פיננסיים, רפואי, למחשב האישי, וכדומה. מומלץ להשתמש בסיסמאות חזקות (שמורכבות מלפחות 8-10 תווים שונים, שכוללים אותיות גדולות וקטנות, מספרים וסימנים). כמו כן, מומלץ להחליף מדי פעם את הסיסמאות שלכם, על מנת למנוע מצב שבו סיסמאות הגישה שלכם נגנבו. ותזכרו: סיסמאות זה כמו מברשות שיניים – אל תחלקו את זה עם אף אחד, ותחליפו אותם מדי פעם.
4. **סיסמה שונה לכל חשבון:** מלבד שימוש בסיסמאות חזקות, מומלץ מאוד להשתמש בסיסמאות שונות לכל חשבון. דבר זה ימנע או יקשה על גניבת הזהויות (סיסמאות) שלכם.
5. **שימוש במנגנון אימות דו-שלבי:** מומלץ להשתמש במנגנון **אימות דו-שלבי** לכל האתרים והאפליקציות שמאפשרות זאת (לרבות חשבונות הבנק, ביטוח, רפואי, דואר אלקטרוני וכדומה).

6. **שימוש ברשתות חברתיות:** עליכם להיות זהירים בתקופה זו בעת השימוש ברשתות החברתיות. הימנעו מהפצת פייק ניוז והודעות שעלולות להכיל מידע רגיש, וגם היזהרו מלחיצה על קישורים ([לינקים](#)) זדוניים שעלולים להזיק.
7. **שימוש באפליקציות למסרים מיידיים:** בתקופה זו יש לא מעט יוזמות של תרומות והתנדבות. שמרו על ערנות וזהירות, מבחינת מה אתם חושפים (תמונות שעלולות להכיל מידע אישי רגיש), פרטים אישיים (טלפונים, כתובות, סיסמאות וכדומה). כמו כן, תיזהרו גם מלחיצה על קישורים ([לינקים](#)) שעלולים להיות זדוניים.
8. **הגנה על המחשב האישי – חשוב להגן על המחשב האישי בבית.** חשוב להתקין עליו תוכנת הגנה (כגון אנטייורוס), ולדאוג לעדכניות תוכנת האנטייורוס, וגם של עדכונים שוטפים של מערכת ההפעלה.
9. **שמירה על ערנות:** נתבקשתם לבצע פעולה "חריגה/משמעותית" כגון העברה כספית, שינוי פרטים רשמיים, מסירת מידע רגיש וכדומה? לא למהר לבצע זאת. מומלץ לוודא בערוץ נפרד (מייל, טלפון, דרך חברים או מכרים וכדומה) את נכונות ההודעה ואימות הבקשה. להלן מספר דוגמאות:
- קיבלתם הודעה במייל לביצוע פעולה? אז תבדקו טלפונית או באמצעות אפליקציות של הודעות (כגון WhatsApp).
 - קיבלתם הודעה ב-WhatsApp לביצוע פעולה? אז תרימו טלפון לגורם הרלוונטי ותוודאו שאכן מדובר בבקשה לגיטימית.
10. **אם יש ספק – אין ספק:** אם יש לכם ספק לגבי פעולה מסויימת, אז עדיף להימנע מביצוע הפעולה.

אם אינכם בטוחים לגבי משהו, ורוצים להתייעץ, אתם מוזמנים לפנות לאיגוד האינטרנט הישראלי, לקבלת סיוע והסברים.

קו הסיוע של איגוד האינטרנט: 050-8858911

קו דיווחים – פייק רפורטר: 052-5862977

כללי זהירות במדיה החברתית



הכוונה כאן היא לשימוש באפליקציות כגון טוויטר (Twitter), פייסבוק (Facebook), טיקטוק (TikTok), אינסטגרם (Instagram) וכדומה.

השימוש ברשתיות החברתיות יכול לסייע במידה רבה (למשל בסיוע לאיתור נעדרים, מתן עזרה לזולת, פעילויות התנדבות ומתן תרומות לנזקקים, ועוד), אך ישנן גם סכנות רבות שיכולות לארוב לנו מעבר לפינה.

1. **הגדרות פרטיות** - תבדקו ותגדירו את ההגדרות שלכם באופן שמספק לכם רמת פרטיות רצויה. הגבילו את הגישה לפרופיל שלכם ולפרטים האישיים. ניתן להגדיר את הפרופיל שלכם כך שרק אנשים שאתם בוחרים יוכלו לראות את הפרופיל שלכם ואת התוכן שאתם מפרסמים.
2. **היזהרו מקבלה והפצה של הודעות כוזבות (פייק ניוז)** - תבדקו את אמינות המקורות של המידע שאתם רואים ו/או רוצים לשתף עם אחרים, והימנעו מלהפיץ חדשות לא בדוקות. לפי הפצת הודעות, תבדקו מול ערוצי החדשות האם הידיעה נבדקה ופורסמה. עורכי החדשות עובדים במרץ לאמת ידיעות ולפרסם אותם, והסיכוי קלוש שנפלה בידכם הודעה ראשונית לפני פרסומה לידי ערוצי החדשות. הפצת פייק ניוז יכול לגרום לבהלה מיותרת, מה שישרת את האויב. קחו שנייה לפני כל שיתוף/הקלקה והתייעצו עם חברים או גורמים מומחים אם אתם לא בטוחים.
3. **שמירה על סיסמאות** - תשתמשו בסיסמאות חזקות (אורך של לפחות 8-10 תווים שמורכבים מאותיות קטנות וגדולות, סימנים ומספרים). אל תשתמשו באותה סיסמה לכל הרשתות החברתיות ושאר השירותים שאתם צורכים (כגון חשבונות הבנק, ביטוח, רפואי, וכדומה), ותחליפו את הסיסמאות מדי פעם.
4. **שמירה על פרטיות ומניעת הפצה של מידע אישי ברשתות החברתיות** - ברשת האינטרנט, קל מאוד לזייף זהויות ולהקים פרופילים מזויפים שמטרתם לאסוף מידע אישי אודות האזרחים. הימנעו מהפצת מידע אישי רגיש (כגון שמות, טלפונים, מיקומים, כתובות, וכדומה). מידע זה יכול לשמש את האויב ולגרום נזק רב.
5. **היזהרו מהפצה של מידע רגיש (בהיבט הבטחוני) ברשתות החברתיות** - עם ישראל אוהב לעזור ולתרום, אך לפעמים בשוגג, אנחנו מפיצים מידע רגיש (בהיבט הבטחוני) שיכול לשמש את האויב ולהזיק לכוחותינו. הימנעו מלצלם תמונות של אמצעי לחימה (כגון טנקים), כוחות צה"ל (חיילים עם נשקים), בסיסים, וכל פרט מזהה אחר שיכול להעיד על המיקום של כוחותינו. אם אתם רוצים לצלם תמונות, תצלמו אותם מול קיר לבן, ותוודאו שאין שום פרט

מזהה בתמונה (דגל של בסיס, שלט, נופים, או כל פרט מזהה אחר שיכול להצביע על המיקום של כוחותינו).

6. **היזהרו מפרסומים והצעות שונות למתן סיוע, תרומות ופעילויות התנדבות - היזהרו מהונאות.** בעת מלחמה, כולנו מאוחדים ורוצים לעזור. יוזמות שונות קמו במטרה לעודד פעילויות התנדבות ותרומות, וזה מבורך. אבל כפי שציינו, קל מאוד להקים קבוצות כאלו, וליפול קורבן למתקפות של מעילות, הונאות או זליגת מידע רגיש אחר (שמות, פרטי התקשרות, כרטיס אשראי, מיקום של כוחותינו, וכדומה). לפני שאתם ממהרים להיכנס לקבוצות שונות ולתרום מכספכם, תוודאו שהקבוצות והארגונים הללו תקינים. תנסו לזהות חברים משותפים שנמצאים בקבוצה, ולוודא איתם שהכל תקין. מלבד האויב, ישנם גם עברייני רשת רבים שינצלו את המצב לעקוץ קורבנות תמימים.
7. **היזהרו מלחיצה על לינקים שיכולים להיות זדוניים** בהמשך לסעיף הקודם, צריכים להיזהר מלחיצה על לינקים שיכולים להיות זדוניים. אל תמהרו ללחוץ על לינקים למתן תרומות וסיוע. תוודאו היטב האם הקבוצות שהוקמו או הארגון שעומד מאחורי הבקשה, אכן תקינים. תבדקו אם יש לכם חברים משותפים שכבר תרמו ונמצאים בקבוצות, שתוכלו לאשר מולם שהארגון תקין ואין ממה לחשוש. ניתן להיעזר בנספח ג' במסמך זה, וללמוד מספר כללי בטיחות כיצד לזהות לינקים זדוניים או לצפות בסרטונים שפרסמנו בפייסבוק.
8. **הימנעו מלהגיב לטרולים ובוטים** - בעת מלחמה, כוחות האויב מעלים בוטים (תוכנות אוטומטיות שמתוכננות לבצע משימות מסוימות ברשתות החברתיות באופן עצמאי) טרולים (אנשים שמטרתם להציק, לזעזע או להרגיז משתמשים אחרים ברשתות החברתיות) רבים לעורר שיח רב, במטרה לאסוף כמה שיותר מידע שיכול לשמש אותם נגדנו. תנסו להימנע מתגובות בהן יכול להיות שאתם חושפים מידע אישי או רגיש (בטחוני).
9. **היזהרו מ"מאגרי מידע" ציבוריים ומשותפים** - בהמשך להנחיות 4 ו-5, אל תמהרו להזין נתונים רגישים (כגון מידע אישי – שם מספרי טלפון, כתובות, וכדומה) לתוך מאגרי מידע שאינם מוכרים ואינם מנוהלים ע"י ארגון מוכר. גם אם המטרה היא טובה, מאגרים אלו עלולים להיות חשופים לגורמים עוינים. גם הימנעו ממסירת מידע רגיש (כגון מיקומים של כוחות הביטחון, מחסומים וכדומה) אל תוך מאגרי מידע שפתוחים ולא מוכרים.
10. **"אל תעבירו את זה הלאה"** - אל תשתפו יוזמות שאתם לא מכירים מי עומד מאחוריהן (יש המון פייק ניוז ומלחמת תודעה + לוחמה פסיכולוגית), וגם האויב יכול להקים קבוצות ויוזמות כאלה במטרה לאסוף מידע רגיש אודות האזרחים וכוחות הביטחון.

ותזכרו תמיד:
שימוש נכון, ימנע אסון.

כללי זהירות למשתמשים באפליקציית WhatsApp



שימוש באפליקציות למסרים והודעות (כגון WhatsApp) יכול להכיל סיכונים רבים מבחינת היבטי אבטחת מידע והגנת הפרטיות, ולכן חשוב להכיר ולפעול לפי כללי הבטיחות הבאים:

1. **הגדרות פרטיות:** תבדקו והגדירו את הגדרות הפרטיות שלכם באפליקציה בצורה שתשמור על הפרטיות שלכם, כולל ההגדרות של מי יכול לראות את הסטטוס שלכם, התמונה ואת המספר שלכם.
2. **הצטרפות לקבוצות:** תגדירו מראש את האפשרויות של הצטרפותכם לקבוצות דיון. באפליקציית WhatsApp ישנן שלוש אפשרויות:
 - א. **ע"י כולם** – בחירת אופציה זו תאפשר לכל אחד להוסיף אתכם לקבוצות דיון מבלי לקבל מכם אישור מראש.
 - ב. **ע"י אנשי הקשר שלי** – בחירת אופציה זו תאפשר רק לאנשי הקשר שלכם לצרף אתכם לקבוצות דיון (חשוב לזכור, זה גם ללא הסכמה מראש).
 - ג. **ע"י אנשי הקשר שלי מלבד...** – בחירת אופציה זו תאפשר לכל אנשי הקשר שלכם לצרף אתכם לקבוצות דיון, מלבד מספר אנשי קשר שהגדרתם שאסור להם.
3. **הפעלת אימות דו-שלבי:** תפעילו את מנכנון האימות הדו-שלבי באפליקציה. זה יספק לכם גישה יותר מאובטחת לחשבון שלכם.
4. **הימנעות משיתוף מידע אישי:** בדיוק כמו ההנחיות שסיפקנו ברשתות החברתיות, כללי הזהירות חלים גם עבור אפליקציית ה-WhatsApp. אין לדעת מיהם חברי קבוצת דיון מסויימת אליה הצטרפתם (או שצירפו אתכם), ולכן מומלץ לא לשתף בקבוצות שום מידע אישי רגיש (כגון טלפונים, כתובות, סיסמאות, מספרי ת.ז., מספרי כרטיסי אשראי ועוד).
5. **הימנעות משיתוף מידע רגיש (בהיבט הביטחוני):** תימנעו (בעיקר בקבוצות דיון) מלפרסם מידע רגיש (כגון מיקום של פריסת כוחות, חלוקת מזון, שמירה בישובים, וכדומה). האויב מאזין.
6. **היזהרו מלינקים זדוניים:** אל תפתחו קישורים או קבצים שקיבלתם ממקורות לא מוכרים או חשודים, ותהיו חשודים גם לגבי קישורים וקבצים שקיבלתם ממשתתפים בקבוצות דיון שונות שאתם משתייכים אליהם. תזכרו שדי קל להצטרף כיום לקבוצות הדיון, ולא תמיד יודעים מיהם המשתתפים בקבוצה.
7. **שימוש בשיחות מוצפנות:** האפליקציה מציעה הצפנה מקצה-לקצה. תוודאו שההצפנה מופעלת בכל השיחות וההודעות שלכם.

8. **תמנעו משימוש ברשתות אלחוטיות ציבוריות:** בייחוד לצורך העברת מסרים בעלי תוכן רגיש, תימנעו משימוש ברשתות אלחוטיות ציבוריות (כגון בבתי קפה, במלון, בתחנת רכבת או אוטובוס, בשדה תעופה וכדומה).
9. **גיבוי המידע:** תצרו **גיבויים** שוטפים של ההודעות והמידע שלכם באפליקציה, כדי למנוע איבוד מידע במקרה של בעיה טכנית או מתקפת סייבר. ניתן לרכוש חבילות אחסון בענן, ולבצע את **הגיבוי** התקופתי אוטומטית לענן.
10. **עדכונים:** תעדכנו באופן שוטף את האפליקציה שלכם לגרסה האחרונה שקיימת כדי להבטיח שאתם מוגנים מפני פרצות אבטחת מידע ידועות. האפליקציה תתריע לכם מתי שיוצאת גרסה חדשה, וכל מה שעליכם לעשות הוא לאשר את העדכון.

“ ותזכרו תמיד:
שימוש נכון, ימנע אסון. ”

כללי זהירות למשפחות השכולות, החטופים והנעדרים



ליבנו עם המשפחות השכולות, ועם משפחות הנעדרים והחטופים, והכאב גדול מנשוא, אבל יחד עם זאת, אנחנו רוצים לסייע במניעת נזק אפשרי נוסף. האויב השיג מספר רב של מכשירי טלפון ניידים, שבאמצעותם יכולים לגשת למידע אישי, ולנצל ערוצי מדיה שונים להפצת מידע כוזב (פייק ניוז), מעילות והונאות, הפחדה וסחיטה, ועוד.

אז מה ניתן לעשות?

1. **עדכון הבנקים וחברות הביטוח והקפאת פעולות באינטרנט ובנייד:** תפנו לבנקים וחברות הביטוח, ותבקשו להקפיא מיידית פעולות באינטרנט ובטלפון הנייד. תבקשו גם דיווח על כל פעולה.
2. **ביטול כרטיס האשראי:** תבטלו באופן מידי את כרטיסי האשראי.
3. **החלפת סים והחלפת בעלות על המכשירים הסלולריים:** תפנו לחברות הסלולר, ותבקשו כרטיס סים חלופי וגם לקחת בעלות על כל החשבונות. לאחר מכן, תגדירו [אימות דו-שלבי](#) למספר החדש.
4. **הוציא את המספרים מקבוצות WhatsApp או לצאת מהקבוצה:** בצער רב, רצטרנו להוציא את המספרים של הנעדרים, חטופים והקורבנות מקבוצות ה-WhatsApp או לצאת מהקבוצה אם הם היו מנהלי הקבוצה. זה יקטין את הסיכון בניסיונות הונאה, סחיטה, והפחדה.
5. **לעדכן את מערך הסייבר הלאומי (בטלפון 119) על כל מקרה חריג:** תעדכנו את מערכת הסייבר הלאומי על כל מקרה חריג כזה.



ותזכרו תמיד:

שימוש נכון, ימנע אסון.



כללי זהירות לארגונים שמנהלים יוזמות התנדבות ותרומות



בימים קשים אלו, צעות יוזמות פרטיות אשר מנסות לגשר על הפערים הקיימים ולתווך בין אנשים הזקוקים לסייע, לאלו שיכולים ורוצים לתת אותו.

יוזמות אלו הן מבורכות, ולרוב מתבצעות במימד הדיגיטלי (אתר, קישור למסמך, אפליקציה וכו'). לצד היוזמות והברכה שביוזמות אלו, ישנם לא מעט סיכונים חבויים, הן כמי שמרים יוזמה כזו והן למשתמש הבודד/לפרט בבואם לצרוך תוכן או להזין נתונים ליישומים אלו.

להלן מספר כללי בטיחות לשימוש באפליקציית WhatsApp לניהול ותפעול קבוצות דיון:

- **שמירה על פרטיות חברי הקבוצה:** אל תאספו ואל תשתפו באופן חופשי ולא מבוקר שום מידע אישי (שמות, מספרטי טלפון, מספרי ת.ז., כתובת פיזית, וכדומה). כלל זה חשוב מאוד בייחוד במצבים שלא מכירים באופן אישי את כל חברי הקבוצה.
- **הצטרפות לקבוצה:** בתור מנהלים של הקבוצות דיון, אתם יכולים לשלוט מי יכול לצרף אנשים לקבוצות, מי יכול לפרסם וכדומה. תשתדלו לממש את הבקורות הללו בניהול הקבוצה, כדי למנוע גישה לא מורשית לקבוצה, ולמידע אישי או רגיש שיכול להיות מפורסם בקבוצה.
- **הימנעו משיתוף מידע רגיש בהיבט הביטחוני:** מידע רגיש יכול להיות מיקום ותמונות של אזורים של חלוקת אוכל (בהם רואים את הבסיסים, או אמצעי לחימה, או את החיילים, וכדומה), מקומות של שמירה בישובים, ועוד. אם נדרש לנהל בסיס נתונים כזה, תמצאו דרך בטוחה ומאובטחת יותר להעביר את המידע לכל חברי הקבוצה. תזכרו שכל פרט מזהה יכול לשמש את האויב לזהות את פריסת כוחות הביטחון שלנו.
- **היזהרו מהודעות וקבצים חשודים:** היזהרו מתוכן של הודעות וקישורים שמגיעים מחברי הקבוצה, גם אם אתם חושבים שאתם מכירים אותם. קל מאוד להפיץ תכנים וקישורים זדוניים, ולכן אנחנו גם ממליצים לא להפיץ קישורים ממקומות שאינם מוכרים ומזהים שהם לא זדוניים.
- **ניהול הרשאות גישה לקבוצה:** תקפידו על מנהלון ניהול הרשאות ועל הדרך שבה מצטרפים משתמשים חדשים לקבוצות, ומי יכול לפרסם מידע בקבוצה. ניתן למשל להגדיר שרק מנהלי הקבוצה יכולים להפיץ מידע, וזה מקטין את הסיכון לזליגת מידע רגיש או אישי.

כללי זהירות והמלצות לשימוש באפליקציות של מסמכים שיתופיים



לעתים, במסגרת היוזמות, מנהלי הקבוצות והעמותות מנהלים בסיסי נתונים באמצעות שיתוף קבצים (שהינם משותפים לכלל חברי הקבוצה). השיתוף נעשה באמצעות אפליקציות ענן כגון Google Sheet, DropBox, OneDrive, וכדומה.

חשוב לוודא שהשימוש בתוכנות אלו נעשה בצורה מאובטחת על מנת להגן על פרטיות ואבטחת המידע שאגור בתוכם. להלן מקבץ של המלצות וכללי זהירות לשימוש בתוכנות או אפליקציות לשיתוף מסמכים:

- **ניהול הרשאות גישה:** תשתדלו להגדיר הרשאות גישה מינימאליות לכלל המשתמשים, למשל, הרשאות לצפייה בלבד, או הצעת הערות לשינוי (אך לא עריכה בפועל). זה יקטין את הסיכון בשינוי לא מורשה של המידע.
- **גיבוי של המידע:** תשתדלו לגבות באופן שוטף את המידע שלכם. לעתים קרובות, גורמים עוינים, באמצעות מתקפות סייבר מתוחכמות, מצליחים לשבש את המידע או להצפין אותו ולדרוש כופר בתמורה לשחרור המידע.
- **השתמשו בכתובת דוא"ל חדשה/שונה:** אין להצטרף לשירותים הללו באמצעות כתובת דואר אלקטרוני של מקום העבודה שלכם, ומומלץ גם לעשות שימוש בכתובת דוא"ל שונה מזו שאתם משתמשים בד"כ לצרכים אישיים (למשל לגשת לחשבון הבנק שלכם). במידה והחשבון נגנב, זה ימנע או יקטין את הסיכון לגישה לא מורשית וביצוע פעולות זדוניות בחשבונות האישיים שלכם. לדוגמה: אם אתם משתמשים בכתובת מייל של GMAIL לגשת לחשבון הבנק שלכם, אז תפתחו תיבת מייל חדשה ב-YAHOO, לצורך עבודה עם קבוצות התמיכה והתרומה.
- **השתמשו בדפדפנים שונים:** מומלץ גם להשתמש בדפדפנים שונים, ולהפריד בין השימוש האישי, לבין השימוש בקבוצות לניהול היוזמות. למשל, אם בד"כ אתם משתמשים בדפדפן של אינטרנט אקספלורר (Internet Explorer) של מיקרוסופט לצורך גישה לחשבון הבנק שלכם, אז תשתמשו בדפדפן של כרום (Chrome) מבית גוגל, לצורך גישה לתוכנות לשיתוף קבצים.
- **ניהול גרסאות:** קבצים שיתופיים אינם מנהלים גרסאות בצורה יעילה, באופן שבו אם גורם עוין ישנה את הטלפון או הכתובת בעמודה/שורה מסוימת, הדבר לא יעורר חשד אצל רוב האנשים. מומלץ מדי פעם לעבור על הרשימות ולוודא שהמידע שמוזן אכן מעודכן ותקין.

כללי זהירות להורים



הורים יקרים

לאחרונה הופצו ועוד לצערנו ימשיכו להפיץ ולחשוף סרטונים ותמונות קשות של קורבנות וחסופים שלנו. על מנת למנוע מילדנו להיחשף לתכנים המזעזעים, ולשמור על הנפש שלהם, ריכזנו עבורכם מספר טיפים ועיצות שתוכלו לנקוט באופן מיידי.

- **הסירו או הגבילו גישה לאפליקציות השונות:** אם ניתן, עבור הילדים הקטנים יותר, הסירו את האפליקציות השונות (טיקטוק, פייסבוק, אינסטגרם, טלגרם וכדומה), כדי למנוע מהם גישה לתכנים המזעזעים. אם מדובר בילדים גדולים יותר, ואי אפשר להסיר את האפליקציות הללו, אז תנסו להגביל את הגישה אליהם.
- **נהלו שיח פתוח עם הילדים בנושא:** חשוב מאוד שתשבו ותדברו עם הילדים, ותסבירו להם שזה נוראי להיחשף למה שיש באפליקציות האלה וזה יהרוס להם את הנפש ואתם דואגים להם וחייבים לשמור עליהם מפני כל רע.
- **תגיעו להחלטה משותפת:** תגיעו ביחד להחלטה להסיר את האפליקציות האלה, או לפחות להימנע מצפייה בתכנים המזעזעים.
- **אל תשאירו אותם לבד:** תהיו בחלל אחד ביחד, שלא יהיו סגורים לבד בחדר לזמן ארוך מדי. תתנו להם מרחב ותכבדו את הפרטיות שלהם, אבל תבדקו מדי פעם מה קורה איתם.
- **תקשיבו להם ותנו להם להביע את דעתם בנושא:** תנו להם לדבר, תקבלו את הרגשות שלהם מבלי לשפוט. בזמנים כאלו, חשוב מאוד שתחזקו אותם.



ותזכרו תמיד:

שימוש נכון, ימנע אסון.



כללי זהירות לכוחות הביטחון



לכוחות הביטחון היקרים שלנו, רצינו להגביר את המודעות שלכם בנושא חשוב מאוד. נכחנו לדעת שבעידן הרשתות החברתיות, סוכני האויב משתמשים באפליקציות שונות לניתוח תמונות, במטרה להבין את מיקום כוחותינו.

ריכזנו לכם מספר טיפים והמלצות כלליות למנוע זליגת מידע לידי כוחות האויב:

- **תצנזרו את התמונות:** תצנזרו את התמונות שאתם מעלים לרשתות החברתיות או שולחים באפליקציות השונות (כגון WhatsApp או טלגרם). תשתדלו להצטלם ולצלם רק על רקע דברים "סתמיים" כמו קיר לבן.
- **הימנעו מלצלם דברים רגישים:** הצטלמתם על דופן של קנט ברקע? תוודא שלא רואים את כל הכלי, אלא רק חלק מצומצם וסתמי. תוודאו גם שלא רואים שום פרט מזהה אחר (מספר הכוחות, סוג הנשקים, דגל של הבסיס, שילוט, או כל דבר אחר שיכול להעיד על מיקום הכוחות).
- **הימנעו מלצלם פרטים מזהים:** הרבה דברים טריוויאליים יכולים להסביר את מיקום כוחותינו. דגלי יחידות ברקע, שלטים עם מקומות, ואפילו פרטים כמו מיקום השמש (עפ"י הצל). נסו לצלם עם פלאש גם ביום כדי להעלים צל.
- **הורידו הוספת מיקום אוטומטית לציוצים, וגם לתמונות:** הורידו בנייד שלכם את האופציה של הוספת מיקום אוטומטית לציוצים וגם לתמונות.
- **הימנעו מלצלם (אפילו בטעות) אנשים או אתרים רגישים:** החלטתם להעלות פוסט בפייסבוק? אין בעיה, רק תוודאו לפני כן שלא צילמתם בטעות אנשים רגישים, או סד"כ כוחות משמעותי.

ותזכרו תמיד:

שימוש נכון, ימנע אסון.

נספח א' - מילון מונחים

"טרול" – טרולים הם אנשים שמטרתם להציק, לזעזע או להרגיז משתמשים אחרים ברשתות החברתיות. עם עשויים לכתוב הודעות מעציבות, מעליבות או מתקיפות בפורומים, תגובות, אתרי אינטרנט, רשתות חברתיות, ועוד, על מנת לגרום למשתמשים אחרים להגיב בצורה רגשית או להיכנס לוויכוחים.

"בוטים" – בוטים הם תוכנות אוטומטיות שמתוכננות לבצע משימות מסוימות ברשת באופן עצמאי. הם יכולים לבצע מגוון רחב של פעולות, כמו לסרוק דפים באינטרנט, לשלוט בחשבונות ברשתות חברתיות, לשלוח הודעות אוטומטיות, ועוד. בוטים יכולים לשמש למגוון מטרות, כמו ניתוח נתונים, שיווק, ואף פעילות זדונית כמו הפצת דואר זבל, איסוף מידע, הסתה ועוד.

"לינק" – מילה לועזית להפנייה או קישור לאתר אינטרנט. זה מאפשר למשתמשים לנווט בין דפים ומשאבים שונים ברשת האינטרנט.

"אימות דו-שלבי" – מדובר בשיטת זיהוי ואימות חזקה, שידועה גם בשם FA2 (ר"ת של 2 Factors Authentication), שיטה שבה נדרשים שני מקדמי זיהוי על מנת לאמת את זהותו של משתמש בעת הגישה לחשבון או לשירות מסוים ברשת. דוגמאות לשני מקדמי זיהוי הינם "משהו שרק המשתמש יודע" (כגון קוד או סיסמה), ו"משהו שנמצא רק בבעלותו של המשתמש" (כגון טלפון נייד או טוקן – שזה אמצעי אבטחה פיזי). למעשה, שיטת אימות דו-שלבי עובדת בצורה כזאת:

- שלב ראשון – המשתמש מזין את שמו ואת סיסמתו באתר או באפליקציה.
- שלב שני – המשתמש מקבל הודעה לטלפון הנייד שלו עם קוד אימות זמני שנשלח בהודעת טקסט (SMS), והוא נדרש להזין את קוד האימות הזמני באתר או באפליקציה כדי להשלים את תהליך הזיהוי ואימות, וכניסה לאתר או לאפליקציה.

"מנגנון CAPTCHA" – ר"ת של Completely Automated Public Turing Test to Tell Computers and Humans Apart. מדובר במנגנון הגנה שמטרתו לוודא שהמשתמש הוא אדם ולא בוט (תוכנה אוטומטית). המנגנון משמש למניעת הונאות ופעילות זדונית באתרים ובשירותים ע"י בוטים שמבצעים פעולות אוטומטיות, כמו שלית דואר אלקטרוני, יצירת חשבונות באופן אוטומטי, הפצת תוכן פרסומי, ואף פעולות זדוניות כגון הפצת מידע כוזב, איסוף נתונים רגישים, ועוד.

אימות רב-גורמי (MFA) – ר"ת של **Multi-Factor Authentication**. זהו תהליך של אימות זהותו של אדם, שמתבסס על לפחות שני אמצעי זיהוי ואימות, השייכים לקטגוריות הבאות:

- ידע (משהו שרק המשתמש יודע – למשל סיסמה), חזקה (חפץ ייחודי שנמצא בחזקתו של המשתמש – למשל מכשיר הטלפון הנייד שלו), וטבועה (משהו שהוא חלק מטבעו הביולוגי וייחודי רק לו – למשל אמצעי ביומטרי כגון אצבע, כף יד, קול, זיהוי פנים, ועוד). **אימות דו-שלבי (2FA)** הינו דוגמה לאימות רב-גורמי.

תקיפות סייבר למטרות השפעה ותודעה – מה שידוע במונח המקצועי כ-**CNI** (ר"ת של **Computer Network Influence**). מדובר במתקפת סייבר שמטרתה לגרום להשפעה תודעתית למשל ע"י השחתת אתר אינטרנט, האלעת אתרים מזוייפים והפצת פייק ניוז, ועוד.

"גיבוי" – פעולה חד פעמית או שוטפת (אחת ליום, אחת לשבוע או לחודש), של העתקת מידע ממוחשב למקום אחר, לצורך מתן אפשרות לשחזורו במקרה שהוא נמחק או שובש. את הגיבוי ניתן לאחסן במחשב, התקן חיצוני נתיק (כגון דיסק קשיח נייד), סביבת ענן, ועוד. דוגמאות לגיבוי בענן, זה כאשר משתמש שומר את המידע שלו בענן (כגון תמונות).

נספח ב' – כיצד ניתן לזהות האם מדובר בלינק (קישור לאתר אינטרנט) זדוני?



זיהוי [לינקים](#) זדונים ברשתות חברתיות הוא קריטי למניעת הונאות או התפקות סייבר. להלן כמה דרכים לזהות ולהימנע [מלינקים](#) כאלה:

1. **תנסו לבחון את כתובת האתר (URL) –** תבדקו היטב את כתובת האתר של [הלינק](#) או ה-URL (ר"ת של **Uniform Resource Locator**). כתובת URL חשודה עשויה להכיל תווים מוזרים, טעויות כתיב, או להיראות כמו גרסה מעוותת של כתובת אתר אמיתית.
2. **תצוגה מקדימה –** רבות מן הרשתות החברתיות מציעות תצוגה מקדימה של הדף שאליה [הלינק](#) מפנה. הסתכלו על התצוגה המקדימה ובדקו אם היא נראית מקצועית ואמינה. אם יש חשש או ספק, ניתן להיעזר באיגוד הישראלי לאינטרנט (קו סיוע של איגוד האינטרנט – 054-8858911).
3. **תיאור הלינק –** תבדקו האם התיאור שמצוי ליד [הלינק](#) רלוונטי ומתאים לתוכן? [לינקים](#) זדוניים לעתים קרובות מצויידיים בתיאורים מטעים או עם הרבה שגיאות כתיב.
4. **אמינות המפרסם –** תבדקו את המפרסם של [הלינק](#). האם זה חשבון מוכר ומהימן, או חשבון חדש שאינכם מכירים? חיפוש קצר במנועי חיפוש (כגון גוגל) יכול גם לאתר האם מדובר בחשבונות פיקטיביים זדוניים.
5. **בדיקת הכתובת בכלים מקוונים –** ישנם כלים מקוונים שמאפשרים לבדוק את האמינות של כתובת אתר. כלים אלה יכולים להציע מידע על האתר והאם הוא נחשב למזיק או זדוני. אחד מהכלים המפורסמים הינו **VirusTotal**. ניתן להשתמש [בלינק](#) הבא: <https://www.virustotal.com/gui/home/url>
6. **תגובות אחרות –** תקראו את התגובות של משתמשים אחרים [ללינק](#). האם ישנן תגובות שמציינות ש**הלינק** זדוני, או שאנשים לחצו ולא קרה כלום מה שיכול להעורר חשד.

7. **אם יש ספק אז אין ספק** – אם יש לכם ספק, עדיף להימנע מלחיצה על [הלינק](#). במקרה של ספק, ניתן לחפש את הנושא באופן ישיר באמצעות מנועי חיפוש מקוונים (כגון [גוגל](#) או [בינג](#)).
8. הזהירות ובדיקה מיטבית של [לינקים](#) ברשתות חברתיות יכולות לעזור למנוע נזקים ולשמור על בטיחותכם ברשת.