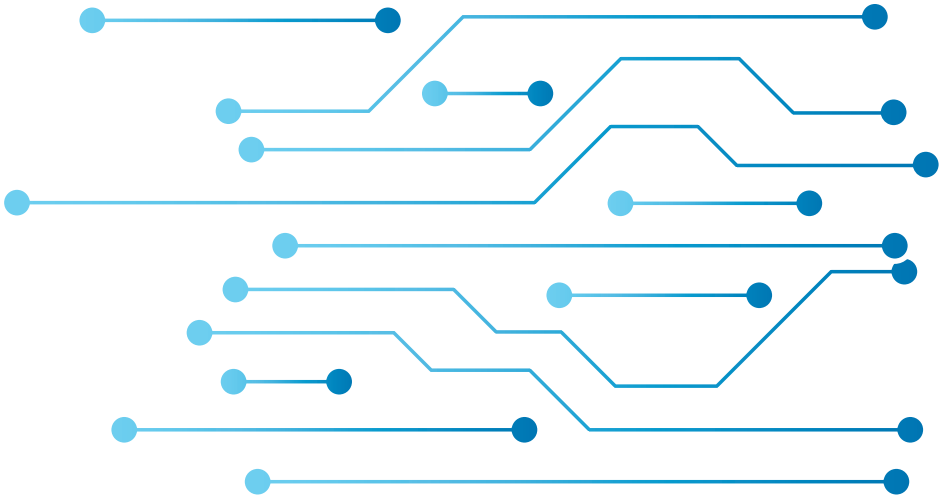
משרד ראש הממשלה
מערך הסייבר הלאומי

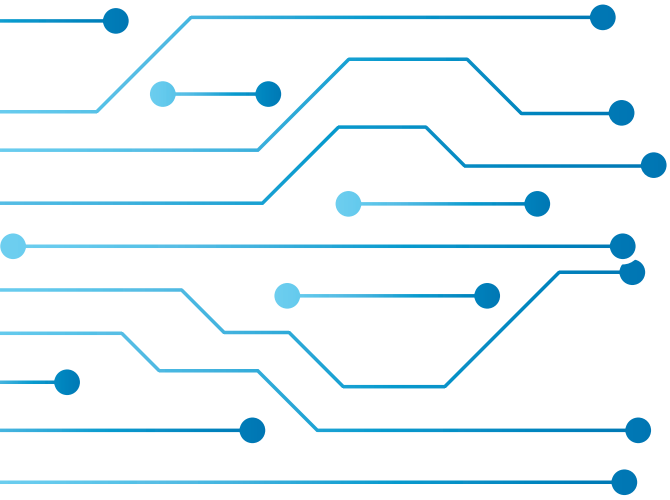
התנהלות בטוחה במרחב הסייבר
להעלאת חוסן תהליך הבחירות בישראל

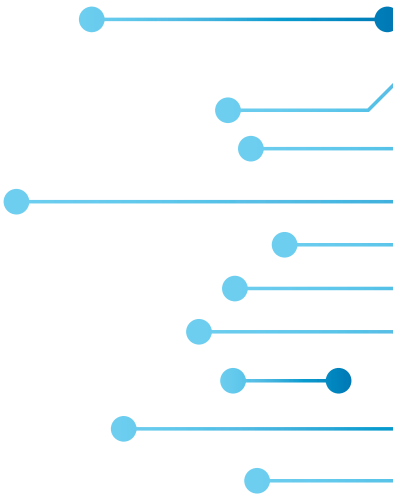
מערך הסייבר הלאומי



משרד ראש הממשלה
מערך הסייבר הלאומי

התנהלות בטוחה במרחב הסייבר
להעלאת חוסן תהליך הבחירות בישראל





תוכן העניינים

מבוא 7

פרק 1
איומי הסייבר האישיים - שיטות תקיפה נפוצות 10

פרק 2
הגדרת רמת הגנה לתוכנות ועדכונן 18

פרק 3
סיסמאות ובקרת גישה 20

פרק 4
הגנה על מחשב נייד ונייח 24

פרק 5
הגנה על דואר אלקטרוני 27

פרק 6
הגנת פרופיל אישי ברשתות חברתיות 30

פרק 7
הגנה על סמארטפונים ושעונים חכמים 32

פרק 8
הגנה על אתר האינטרנט 36

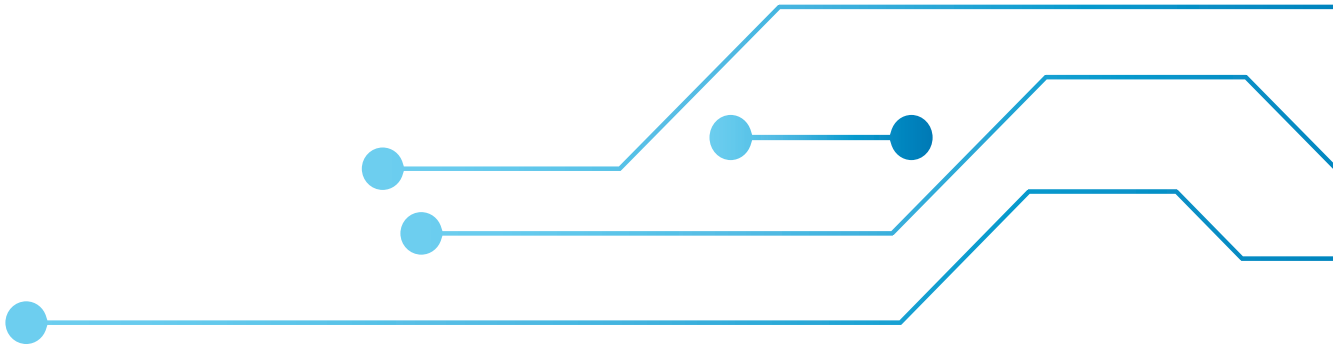
פרק 9
גיבוי ויכולת התאוששות 40

פרק 10
התנהלות בטוחה 42

פרק 11
מה לעשות במידה והותקפת? 44

"עשרת הדיברות" להתנהלות בטוחה 46

*המדריך כתוב בלשון זכר אך מיועד לנשים ולגברים כאחד.



מבוא

דמוקרטיה היא שיטת ממשל בה לצד זכויות הפרט, יש לאזרחים יכולת להשפיע על המדיניות הציבורית במדינתם, באופן חוקי וממוסד. ביטוי השיא ליכולת זו ולהליך הדמוקרטי הינו קיומן של **בחירות כלליות**, חופשיות, חוזרות ונשנות במרווחי זמן הנקבעים בחוק. גם בישראל מערכת הבחירות מהווה את אחד מעמודי התווך של המשטר הדמוקרטי במדינה, ונערכת תוך שמירה על עקרונות היסוד של שיטת הבחירות בישראל ובהם השמירה על החשאיות וטוהר הבחירות. טוהר הבחירות מחייב שכל בוחר המממש את זכותו להצביע, עשה כן כבן-חורין ועל-פי שיקול דעתו החופשי.

שמירה על עקרונות אלו מהווה מרכיב מרכזי בבניית **אמון הציבור במדינה** ואמון האזרחים במוסדותיה.

בשנים האחרונות אנו עדים ל**ניסיונות התערבות חיצונית** ולפגיעה בהליכי הבחירות ובתוצאותיהן במדינות דמוקרטיות רבות בעולם, באמצעות תקיפות במרחב הסייבר[1]. ניסיונות אלו ניתן לסווג לשני מרחבי פעולה עיקריים: המרחב האחד הינו **פגיעה בהליך הבחירות עצמו**, באמצעות פגיעה במערכות המידע, מערכות ההצבעה וספירת הקולות, סדר ההגעה לקלפיות, מערכות הסיקור וכו'. המרחב השני הינו **תודעתי**, ומכוון להשפעה על הבוחרים באמצעות פגיעה בשמם הטוב של מועמדים וערעור באמון הציבור במוסדות הדמוקרטיים, לעיתים קרובות באמצעות השגת מידע או שיבושו על ידי תקיפות סייבר, ושימוש בו לאחר מכן באמצעי הפרסום והמדיה השונים, לרוב באמצעות ערוצי המדיה החברתית או באמצעות אתרים שמתמחים בחשיפה (דוגמת WikiLeaks).

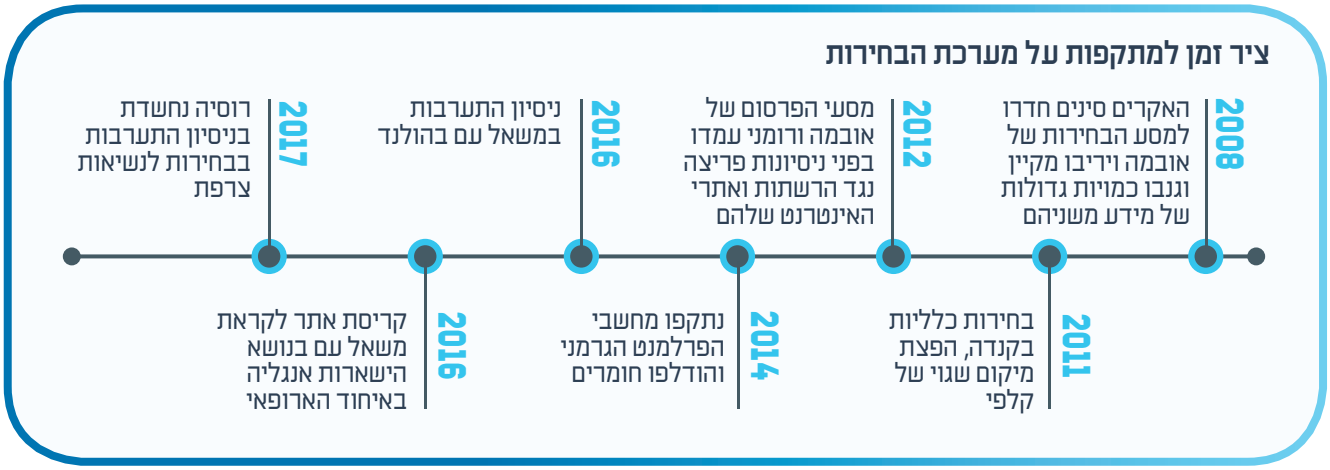
במדינות אריזונה, ג'ורג'יה ואילינוי שבארצות הברית התבצעו ניסיונות תקיפה למאגרי המידע הדיגיטליים, אשר עלולות היו להביא לגניבה או חשיפת פרטיהם של כ–21 מיליון אזרחים אמריקאים. לגניבת זהות, הדלפת פרטים ו/או שינוי שלהם יכולה להיות השלכה על ההליך הדמוקרטי כולו. בבחירות הכלליות בקנדה בשנת 2011 קיבלו אזרחים הודעות טלפוניות על מיקום שגוי של קלפי, כנראה במטרה לפגוע במוטיבציה של מצביעים לממש את זכות ההצבעה שלהם.

בשנת 2008 האקרים סינים חדרו למסע הבחירות של אובמה וירבו מקיין והצליחו לגנוב כמויות גדולות של מידע משניהם. בשנת 2012, מסעי הפרסום של אובמה ורומני עמדו בפני ניסיונות פריצה נגד הרשתות ואתרי האינטרנט שלהם. בשנת 2014 נתקפו מחשבי הפרלמנט הגרמני (בונדסטאג) והודלפו חומרים מפלגתיים רבים. התוקפים מעולם לא זוהו, אך נראה כי חלק מחומרים אלו שימשו בשנים הבאות לקמפיינים של התססה ושנאת זרים במדיה החברתית בגרמניה.

ב-2016 התקיים ניסיון להתערבות במשאל העם שהתקיים בהולנד, שנערך בעקבות דרישה לבטל את הסכם הסחר של האיחוד האירופי עם אוקראינה, והמיוחס לרוסים. בעקבות ניסיון זה, החליטו ההולנדים לחזור לשימוש בקלפיות נייר מסורתיות בבחירות לפרלמנט שהתקיימו כעבור שנה.

---

1 להרחבה: דודי סימן טוב, גבי סיבוני וגבריאל אראל, "איומים קיברנטיים על תהליכים דמוקרטיים", המכון למחקרי בטחון לאומי (INSS), סייבר, מודיעין ובטחון, 1(3), עמ' 59-69, דצמבר 2017,
http://www.inss.org.il/he/wp-content/uploads/sites/2/2017/12/CyberHEB1.3_5.pdf



דו"ח קהילת המודיעין של ארה"ב מ-2017 מעריך כי התקיימה פעילות רוסית נרחבת בבחירות האחרונות בארה"ב באמצעות תקיפות סייבר, כולל שימוש במידע שנגנב מפריצה שביצעו הרוסים למחשבי המפלגה הדמוקרטית האמריקאית החל מיולי 2015 (ניסיונות תקיפה התקיימו כנראה גם כלפי המפלגה הרפובליקנית). בנוסף, השיגו האקרים גישה לחשבון דוא"ל של עוזר בכיר למועמדת הדמוקרטית. החומרים שהושגו בפריצות אלו הודלפו, לעיתים בצורה מגמתית ותוך שיבושים, וזכו לחשיפה נרחבת בתקשורת ובמדיה החברתית. למידע זה נודעה השפעה משמעותית על ירידת מידת אמון הציבור בטוהר המערכת הפוליטית ובתקינות הליך ההצבעה, ויש הטוענים כי אף השפיעה על תוצאות הבחירות.

רוסיה נחשדה גם בניסיון להתערבות בבחירות האחרונות (2017) לנשיאות בצרפת, אשר מטרתו הייתה לפגוע בסיכויי בחירתו של עמנואל מקרון, זאת באמצעות פרסום מידע (שייתכן וחלקו זויף) אשר נגנב ממטה הבחירות שלו.

ב-2016 נחשף בראיון לעיתון אדם פרטי שעמד לטענתו בראש צוות האקרים-שכירים אשר הופעלו ע"י גורמים פוליטיים במספר מדינות בדרום-אמריקה, במטרה להטות את תוצאות הבחירות. הנ"ל תיאר כיצד צוותו התקין תוכנות ריגול במחשבים של יריבים, גנב את התוכניות האסטרטגיות של היריבים, וביצע מניפולציות שונות במדיה החברתית.

ביום ה-23 ביוני 2016 התקיים בבריטניה משאל עם בשאלת ההישארות או העזיבה של בריטניה את האיחוד האירופי. ע"פ דו"ח של וועדת[2] בית הנבחרים הבריטי בנושא, ב-7 ביוני קרס אתר ההרשמה[3] להצבעה במשאל העם, שעות ספורות בטרם הוא נסגר לרישום להצבעה. הוועדה ציינה כי יש אינדיקציות שקריסת האתר נגרמה בשל מתקפת מניעת שירות מכוונת[4] (DDOS), ייתכן באמצעות bot-ים[5], וכי התזמון וההיקף הם אינדיקציה לכך שייתכן ומדובר במתקפה מכוונת.

ההבנה כי קיימת עלייה בשימוש באסטרטגיה זו מחייבת הרחבת ההתגוננות במדינה דמוקרטית נגד איום זה. ניצול חולשות אנושיות הוא המקור העיקרי להתקפות סייבר - **כל אחד מהגורמים השונים המעורבים במערכת הבחירות עלול להיות, לרוב ללא ידיעתו, יעד למתקפה או "שער כניסה" למתקפה על אחרים.** כך למשל,

2 הוועדה למנהל ציבורי ועניינים חוקתיים.
3 אתר ההרשמה אפשר למי שהיה זכאי ומעוניין להצביע, ושפרטיו לא היו מצויים ברשות המדינה, להירשם להצבעה.
4 ראה הסבר על מתקפת מניעת שירות בפרק 1.
5 ראה הסבר על bot-ים בפרק 6.

הנגישות לדוא"ל של המועמדת הדמוקרטית לנשיאות הילארי קלינטון לא הושגה באמצעות גישה לחשבון הדוא"ל שלה, אלא באמצעות חשבון הדוא"ל של אחד מעוזריה הבכירים. דבר זה מחייב כל אחד ואחת לרכישת ידע בסיסי, לגילוי ערנות ואחריות אישית וארגונית ולביצוע פעולות הגנה בסיסיות.

מדריך זה נכתב במטרה לחשוף בפניכם את הסיכונים, להעלותם למודעות ולסייע לכם בקבלת כלים ואסטרטגיות להגנה אישית וארגונית. במדריך נפרט מספר שיטות ואמצעים שבאמצעותם ניתן לאבטח, להקשות או למנוע מגורמים עוינים לחבל במערכת הבחירות. מטרת המדריך לסייע ב"חיסון" נקודות התורפה על מנת להקשות על ההאקרים ולהפחית את הסיכונים לפגיעה. כמובן שאין צורך להיות מומחה סייבר על מנת לנהל קמפיין בחירות מוצלח, אך בהחלט ישנה אחריות רבה להגן במרחב הסייבר (הזירה הדיגיטלית) על ההליך הדמוקרטי, המועמדים והארגון מפני היריבים. **כממלאי תפקידים משמעותיים בתהליך הבחירות, חשוב שתכירו את האיומים על מרחב הסייבר האישי שלכם והדרכים המומלצות להתמודד איתם.**

מדריך זה נכתב עבור כלל המעורבים והמשפיעים במערכת הבחירות ולסביבתם הקרובה.

מטרת המדריך:

- לתאר את האיומים במרחב הסייבר האישי - שיטות התקיפה הנפוצות
- לציין מהם האמצעים הבסיסיים שניתן לנקוט על מנת להקטין את הסיכוי שתותקפו דרך מרחב הסייבר
- להנחות כיצד להתמודד מפני פגיעת היריבים בהליך הדמוקרטי של הבחירות ובהתנהלות יומיומית בטוחה בבית ובמשרד, בהגנה על מחשבים וטלפונים סלולריים, בהגנה על המידע ברשתות החברתיות, באתר האינטרנט האישי ובדואר האלקטרוני
- לאפשר לכלל נותני השרות, כולל אלו ללא כל הכשרה טכנית, להבין וליישם את האמצעים הבסיסיים להגנה שיסייעו בהגברת האבטחה מפני פגיעת היריבים בהליך הדמוקרטי של הבחירות
- לצמצם נזק שעלול להיגרם לתהליך הבחירות הדמוקרטי

מערך הסייבר הלאומי הנו יחידת סמך במשרד ראש הממשלה, אשר אמון על הגנת מרחב הסייבר הלאומי ושיפור החוסן המדינתי. מערך הסייבר מסייע ומייעץ לוועדת הבחירות המרכזית לבקשתה, וכן לקצין הכנסת, במגוון ערוצים על מנת לאפשר תהליך בחירות חופשי מהשפעה של תקיפות במרחב הסייבר.

למידע נוסף והרחבות למנהלי אבטחת מידע, ניתן לעיין בתורת ההגנה בסייבר לארגון.[6]

6 https://www.gov.il/he/Departments/Guides/cyber_security_methodology_for_organizations_test

פרק 1

איומי הסייבר האישיים - שיטות תקיפה נפוצות

מרחב הסייבר האישי מוכר לכולנו היטב. אתר אינטרנט אישי, דואר אלקטרוני פרטי ודואר אלקטרוני ארגוני, טלפון סלולרי, רשתות חברתיות - כל אלו כלים יומיומיים המשמשים אותנו לטובת העבודה ומהווים חלק חשוב בשמירת קשרים מקצועיים, אישיים וחברתיים.

התנהלות בטוחה במרחב הסייבר תאפשר לנו ליהנות מהיתרונות הטכנולוגיים, תוך צמצום הסיכון שניפגע דרך מרחב הסייבר האישי. הדבר נכון לכל אזרחי המדינה, אבל הוא מקבל משנה תוקף לגביכם - האנשים המעורבים בצורה ישירה והמשפיעים בצורה משמעותית במערכת הבחירות בישראל. **כאמור, אתם עלולים להוות מושא תקיפה ברמה האישית** לטובת איסוף המידע המצוי ברשותכם ובמטרה לפגוע בכם במרחב הסייבר (פריצה לדוא"ל האישי, השחתת דף המדיה החברתית שלכם וכד'), **כאמצעי לפגיעה בארגון שלכם** (הארגון או המפלגה למשל) **או לפגיעה בתהליך הבחירות עצמו.**

מי הגורמים המאיימים עליכם במרחב זה?

גורמים רבים יכולים לאיים במרחב:

גורמים אלו עלולים **לחשוף מידע רגיש** המצוי אצלכם או בארגון שלכם, **להשבית** או **לשבש** את תהליך הבחירות התקין, **להשחית** מידע בעל השפעה חיונית בתהליך הבחירות ותוצאותיו ועוד.

שיטות תקיפה נפוצות

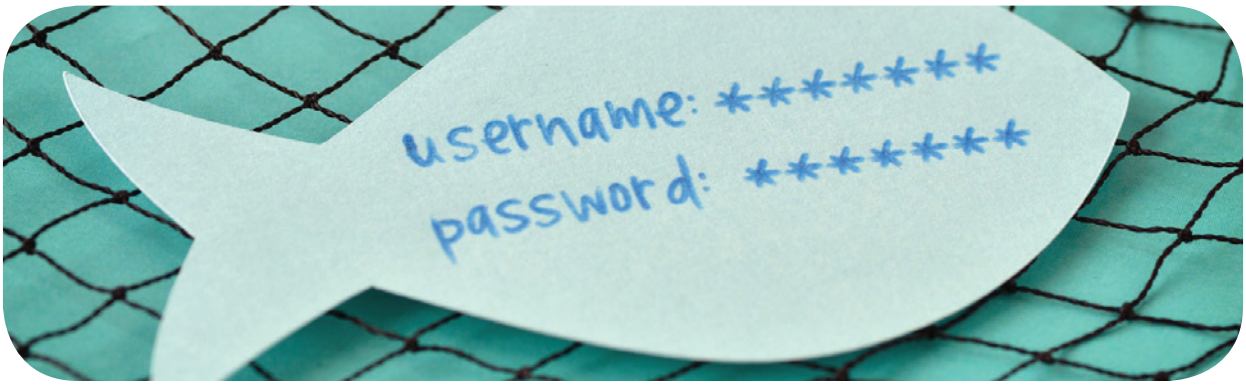
<u>תקיפות "הנדסה חברתית"</u>

■ **"הנדסה חברתית"** משמעה ביצוע **מניפולציה** על הנתקף, באמצעות ניצול מנגנוני ההתנהגות של האדם המצוי. באמצעות מניפולציה זו הפורץ מצליח **לשכנע** את האדם לבצע פעולה (לדוגמה: להעביר לו פרטים אישיים/מידע, או להפעיל תוכנה זדונית), וכך הוא עוקף את כל מנגנוני האבטחה.

הרעיון של הנדסה חברתית אינו חדש וקיים כבר אלפי שנים - אם נחשוב על רמאים או נוכלים, עצם הרעיון זהה - אולם הטכנולוגיה של היום יעילה יותר באופן דרמטי עבור התוקפים, משום שהנתקף לא יכול לראות אותם פיזית והם יכולים בקלות להתחזות למישהו אחר. התוקף גורם לנתקף לחשוב שהוא מתקשר עם גורם לגיטימי עליו הוא סומך, בעוד שבפועל הנתקף, ללא ידיעתו, למעשה פועל למול צד ג' עוין.

כלומר, באמצעות "הנדסה חברתית" הנך עלול, ללא ידיעתך, לאפשר לגורם עוין להיכנס לרשתות הארגון/מפלגה/לאמצעים הפרטיים שלך ולהוביל לנזקים משמעותיים.

■ **דיוג - 'פישינג'** (Phishing) - אחת משיטות התקיפה של "הנדסה חברתית" והנפוצה שבהן. בשיטה זו מטרת התוקף הינה "להעלות בחכתו" גורמים בכירים וזוטרים, וע"י הטעיה, הפחדה או פיתוח ציפיות, לפתותם לבצע פעולה בעלת מוטיבציה נסתרת זדונית.



דוגמאות למניפולציות:

- מסמך הנראה לגיטימי לכאורה - כגון חשבונית או קבלה (invoice, receipt) - המתקבל ממקור לא מוכר, או בעל סימנים מחשידים[7].
- הודעה על סיסמה פגת תוקף (המציעה לנתקף להחליף סיסמה) או דרישה לאימות פרטי חשבון.
- הצעה שיווקית קוסמת, מוצר נחשק במחיר מפתיע או זכייה בפרס כספי. פעמים רבות ההצעה נראית טובה מדי מכדי להיות אמיתית, כמו "אייפד חינם בכל קניה" או מוצרים נחשקים במחירים בלתי הגיוניים.
- הודעת אזהרת אבטחה (Security Alert) - הודעה המתריעה לכאורה על פריצת אבטחה, המציעה לנתקף להחליף סיסמה.

כאשר בפועל בכל אחד מהמקרים הנ"ל, מדובר בהודעה מתחזה מתוקף.

7 סימנים מחשידים - לדוגמה, נושא שאינו בהכרח קשור לשולח או לסוג ההתקשרות, שגיאות כתיב מוזרות

- **דיוג ממוקד (Spear Phishing) - שליחת הודעה ממוקדת לאדם ספציפי או קבוצה ממוקדת.** בניגוד להתקפת דיוג, המבוצעת כאשר התוקף פונה לתפוצה רחבה של אנשים (בדומה להטלת רשת של דייג), **דיוג ממוקד** מתמקד ומותאם אישית למספר קטן מאוד ונבחר של אנשים, לאחר שהתוקף אוסף עליהם מידע ואף לעיתים מצליח לחדור למערכות הארגון. לכן פניה מניפולטיבית לנתקף מסוג דיוג ממוקד תהיה לרוב **מאוד מציאותית וקשה לזיהוי**. לעתים קרובות היא תגיע מכתובת שתראה כמו כתובת של גורם מוכר או קולגה, היא עלולה להשתמש באותה שפה או בסלנג אשר הקולגות שלך משתמשים בהם, בלוגו של הארגון שלך או אפילו בזיוף החתימה הרשמית של מנהל בכיר בארגון. הודעת דיוג ממוקד עשויה אפילו להיראות כמענה לתכתובת אמיתית שניהל המקבל עם שולח ההודעה. פניות אלו לעתים קרובות יוצרות תחושה עצומה של דחיפות, הדורשות ממך לנקוט בפעולה מיידית ולא לספר לאף אחד.

- **דוגמאות לפעולה שמתבקש הנתקף לבצע - והפעולות הזדוניות המסתתרות מאחוריה:**

לחיצה על קישור שנראה כאילו הוא מוביל לאתר "לגיטימי" אך בפועל מדובר באתר מתחזה - באתר המתחזה הנתקף יתבקש להזין את פרטיו האישיים (כגון ת.ז., שם משתמש, סיסמה). המניפולציה שבוצעה מפתה את הנתקף להזין פרטים אלו - אשר מאפשרים לתוקף לנצלם למטרותיו, כגון להיכנס לחשבון של הנתקף (למשל לחשבון האימייל).
בנוסף, עקב חוסר מודעות אנשים רבים נוהגים להשתמש באותה סיסמה בכל החשבונות שלהם - וכך, אם התוקף השיג את סיסמת ה-Facebook שלהם, פעמים רבות היא תשמש אותו גם לחשבון הדוא"ל שלהם, חשבון הבנק ועוד.

לחיצה על קישור המוביל לאתר לגיטימי, אך בפועל גם תותקן נוזקה ללא ידיעת הנתקף - הלחיצה על הקישור תגרום לכך שתחילה יבוצע Download לנוזקה אל מחשב הנתקף, ורק אז יופנה הנתקף לאתר. נוזקה זו תאפשר למשל השתלטות מרחוק של התוקף, או תשלח אליו מידע פרטי של הנתקף. לעיתים תפעל הנוזקה כ"ראש גשר" המאפשר לתוקף לשכפל את המתקפה - למשל, הנוזקה תשלח את הקישור לכל אנשי הקשר של הנתקף, וכך "תדביק" במהירות את כל הארגון. פעולת ה-Download תבוצע בפרק זמן כה קצרצר, עד שהנתקף כלל לא יוכל להבחין בכך.

פתיחת מסמך או קובץ "לגיטימי", אך בפועל תותקן נוזקה ללא ידיעת הנתקף - בדומה, פתיחת הקובץ תגרום לכך שיבוצע ברקע Download לנוזקה אל מחשב הנתקף והתקנתה, כאשר הנתקף לא מודע לכך כלל.

■ פלטפורמות דיוג נפוצות:

דואר אלקטרוני - אפקטיביות השיטה נובעת **מקלות שליחת המיילים**, המאפשרת לתוקף **תפוצה רחבה בעלות נמוכה** יחסית, וכן מספיק כי **אחוז קטן** מאוד מהנמענים ייענה להצעות בכדי שהתוקף יקבל את המידע שהוא צריך. בדיוג ממוקד יראה הדואר כתכתובת רגילה ולגיטימית עם אחד מאנשי הקשר הקבועים של מקבל ההודעה. להודעה מעין זו עשוי להיות מצורף קובץ או קישור ואפילו כזה שנשלח בעבר בין הצדדים (למשל: "מצ"ב הערותיי למסמך ששלחת בשבוע שעבר...")

הודעת טקסט - (סמישינג - פישינג באמצעות הודעת SMS או WhatsApp). התוקף עשוי לשלוח טקסט הקורא לפעולה לגיטימית, בתוספת קישור לכתובת אינטרנט. דוגמאות לכך: רישום לאירוע, ביצוע תשלום, קבלת משלוח, מבצעים אטרקטיביים, הורדת אפליקציה.

מודעת פרסומת - באתרים באינטרנט (כגון באתרי חדשות), או במדיה חברתית (כגון Facebook). בלחיצה על המודעה נגיע למשל לאתר מתחזה.

שיחת טלפון (Voice Phishing) - לדוגמה, הנתקף מקבל שיחת טלפון מאדם הטוען שהוא מתמיכת המחשוב של הארגון, ספק שירותי האינטרנט או אולי מהתמיכה הטכנית של ספק שירותי הסלולר. המטלפן מסביר כי זוהתה פעולה חשודה במחשב של או בטלפון הנייד של הנתקף, וכי הוא מעוניין לסייע לו לאבטח את המחשב. התוקף משתמש במגוון של מונחים טכניים בכדי לבלבל את הנתקף ובכך מצליח לשכנע אותו למשל לתת לו את פרטי שם המשתמש והסיסמא שלו, או להתקין לו מרחוק תוכנת עזר (אשר בפועל היא נוזקה).

■ את מי יתקפו?

פעמים רבות ישנה נטייה לחשוב כי התקיפה תכוון כנגד בכירים, או כנגד מי שמחזיק בעמדות מפתח. בפועל לרוב התקיפה תהיה מכוונת להשיג נגישות למערכות המחשב או נגישות למידע, ועל כן יעד לתקיפה יכול להיות כל אחד שיש לו גישה למערכות המידע בארגון או למידע עצמו: המאבטח, העוזר, המזכיר, העובד הזוטר.

■ היכן תבוצע התקיפה?

לרובנו קיימים שורה של חשבונות ושירותים דיגיטליים **פרטיים** (דוא"ל, רשת חברתית), ובמקביל שירותים דיגיטליים **ארגוניים** (דוא"ל משרדי). בפועל, לרוב מתקיים **ערבוב** בין השניים: אנחנו פותחים את דף הגישה של חשבון ה-Gmail במשרד, ניגשים לדוא"ל הארגוני דרך הטלפון הנייד הפרטי, משתמשים לעיתים בדוא"ל הפרטי לצורך ארגוני או להיפך. לכן חשוב להדגיש כי התקיפה יכולה להתבצע כנגד החשבונות הפרטיים, כמו גם כנגד החשבונות הארגוניים. נוסיף לכך את העובדה שהרשת החברתית הפרטית מאפשרת לאסוף מידע חשוב על הנתקף לצורך הנדסה חברתית.

■ מתי תבוצע התקיפה?

בעת תקיפת סייבר, לרוב יידרש התוקף לזמן ארוך לשם מימוש ההישג בחדירה לרשת (למשל: איסוף מידע לאורך זמן). על כן, אין לצפות כי תקיפות סייבר יבוצעו בסמוך לתאריך יעד כגון מועד הבחירות, אלא יש לצפות להתרחשות התקיפה בכל רגע, ואף זמן ממושך מאוד לפני מועד הבחירות. בתקיפות מוכרות בוצעה פעמים רבות החדירה הראשונית לרשת בפרקי זמן של 12-24 חודשים לפני "תאריך היעד".

■ כיצד תוקף יכול לגרום לנזק באמצעות תקיפות אלו?

בדרכים רבות. דוגמאות:

גניבת פרטי ההזדהות (שם משתמש וסיסמא), או פרטים אישיים אחרים (מספר ת.ז. או מספר כרטיס אשראי).

באמצעות פרטי ההזדהות שלך התוקף יכול לגנוב את הזהות שלך ולפרסם הודעות שקריות בשמך (Fake news) ברשתות החברתיות.

לקרוא (ולהעתיק) הודעות רגישות שנשלחו אל החשבון האישי שלך בדוא"ל.

להדליף תכתובות ומידע עסקי/פוליטי/רגיש אשר שיתפת בקבוצה "סגורה" או באופן פרטי.

להאזין לך ולהקליט אותך.

לפגוע במוניטין שלך באמצעות פרסום מידע מביך ואישי.

לסכן אותך בעבירה על חוק הגנת הפרטיות או חקיקה/תקינה אחרת כתוצאה מפרסום מידע רגיש בשוגג.

לחדור דרכך אל הארגון שלך, ל"הדביק" גורמים נוספים בארגון, עד להשבתת כל המחשבים שבו ללא יכולת לגשת למידע האגור בהם.

לבצע מעקב פיסי באמצעות מיקום סלולארי. אפשרות לדעת בכל רגע נתון את מקום הימצאותך.

לשבש מידע.

תקיפות נפוצות נוספות

השחתה (Defacement) של אתר האינטרנט/דף מדיה חברתית -

- **מהי השחתה?**

תקיפה של אתר אינטרנט/דף מדיה חברתית (כגון דף ה-facebook או ה-twitter), אשר מטרתה **לשנות את התוכן** באתר (לרוב את דף הבית), בתוכן המשרת את מטרות התוקף. בעקבות ההתקפה חלים שינויים בפני האתר, ובמקום עמוד בית תקין מופיעים לרוב משפטי נאצה, סיסמאות פוליטיות, או כל מסר אחר שהפורץ מעוניין להעביר.

- **מהו הנזק הפוטנציאלי מתקיפות מסוג זה?**

> מטרות תודעה ותעמולה
> פגיעה במוניטין, תדמית
> לעיתים המטרה היא הסוואה - כאשר משחיתים בגלוי אתר של ארגון, הוא מיד מודע לכך, מתמודד עם התקיפה ומשפר את הטעון שיפור, ולאחר מכן הוא משוכנע שהוא מוגן - אלא שאינו מודע לכך שבמקביל, התקפה משמעותית יותר מתנהלת מכיוון אחר והארגון לחלוטין אינו מוגן.

- **כיצד התקיפה מתאפשרת?**

השחתת האתר מתאפשרת בהינתן הרשאות מתאימות אשר לרוב מושגות ע"י ניצול פרצת אבטחה באתר או בשרת[8].

8 על החשיבות שבביצוע התקנת עדכוני הגנה ראה בפרק 2, הרחבה בנושא אבטחת אתרי אינטרנט בפרק 8.

מתקפת מניעת שירות -

- **מהי מתקפת מניעת שירות?**

תקיפה אשר נועדה להשבית מערכת/אתר אינטרנט, על ידי יצירת עומס חריג על משאביו. למעשה מדובר במשפחה של מתקפות מסוגים שונים, שכל אחת מהן מנצלת פרצת אבטחה אחרת במערכת המותקפת כדי להשיג את האפקט המבוקש.

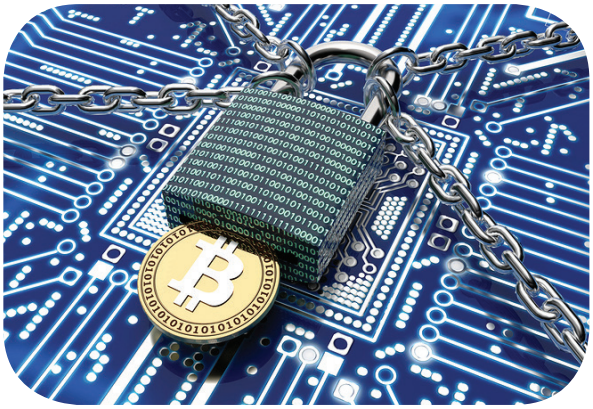
התקפת DOS (Daniel of Service Attack) מתבצעת לרוב באמצעות מחשב אחד המחובר לאינטרנט, אשר תוקף ומציף את השירות המותקף.

התקפות DDOS (Distributed Daniel of Service Attack) מתבצעות לרוב בעזרת כמות גדולה של מחשבים המחוברים לאינטרנט עם מזהים (כתובות IP) שונים, המתקיפים את השירות המותקף בו-זמנית. רשת מחשבים זו מגיעה לעיתים למאות אלפי מחשבים ושרתים ומכונה **בוטנט** (botnet).

- **מהו הנזק הפוטנציאלי מתקיפות אלו?**

מטרת העומס להביא לקריסה או האטה משמעותית של המערכת/אתר. בכך נפגעת **הזמינות** - לדוגמא, אם מדובר באתר, האתר לא יהיה זמין ולא ניתן יהיה לגשת אליו. נזק אפשרי נוסף הוא פגיעה **במוניטין** ופגיעה **תדמיתית**.

מתקפת כופר/כופרה (Ransomware) -



- **מהי מתקפת כופרה?**

התקפה זו מתחילה לרוב בפעולת דיוג. כאמור, אחת הפעולות הזדוניות שתוקף עלול לבצע באמצעות דיוג, היא להוביל להתקנת נוזקה במחשב הנתקף. נוזקה מסוג כופרה מגבילה את גישת המשתמש למערכות המחשב שלו והמידע בו על ידי **הצפנת הקבצים** שעל הכונן הקשיח, תוך הצגת דרישת כופר מהנתקף בכדי להסיר

את ההצפנה. במידה ולא ישולם כופר, למעשה ינוטרל הנתקף מהיכולת לעבוד על מחשבו והמידע שלו אינו נגיש.

תוכנות כופר אחרות פשוט **נועלות** את המערכת ומציגות הודעת שווא כי לא ניתן לגשת לקבצים, על מנת לרמות את המשתמש ולהמריצו לשלם.

לרוב, מרכיב מרכזי בדרישת התשלום הוא שהתשלום יבוצע באמצעות מערכת תשלומים שלא ניתנת למעקב. קיים מגוון רחב של שיטות תשלום, כולל: העברה בנקאית, העברה באמצעות מסרון, ושימוש במטבע וירטואלי (כגון Bitcoin) .

יצוין כי לעיתים קרובות גם תשלום כופר לא בהכרח יוביל את התוקף "לשחרר" את ההצפנה.

- **מהו הנזק הפוטנציאלי מתקיפות אלו?**

במקרה בו הנתקף החליט לשלם את הכופר, והתוקף אכן "שיחרר" את המחשב בתמורה - אזי נגרם נזק כספי.

במקרה בו הנתקף החליט שלא לשלם את הכופר, הוא עלול להסתכן באובדן המידע שלו[9] ואף בהשבתה מפעילות.

בשני המקרים קיים פוטנציאל ל**נזק תדמיתי ולפגיעה במוניטין**.

תקיפות ייעודיות המנצלות חולשות אבטחה במוצרים השונים בהם אנו משתמשים - לליקויי אבטחה אלו ישוחררו לשוק תיקוני אבטחה בידי היצרנים השונים, אולם עד לשחרורם לשימוש הם ניתנים לניצול בידי גורמים עוינים.[10]

9 הדבר מגביר את החשיבות של ביצוע גיבויים - ראה פרק 9.
10 על החשיבות שבביצוע התקנת עדכוני הגנה - ראה פרק 2.

פרק 2

הגדרת רמת הגנה לתוכנות ועדכונן

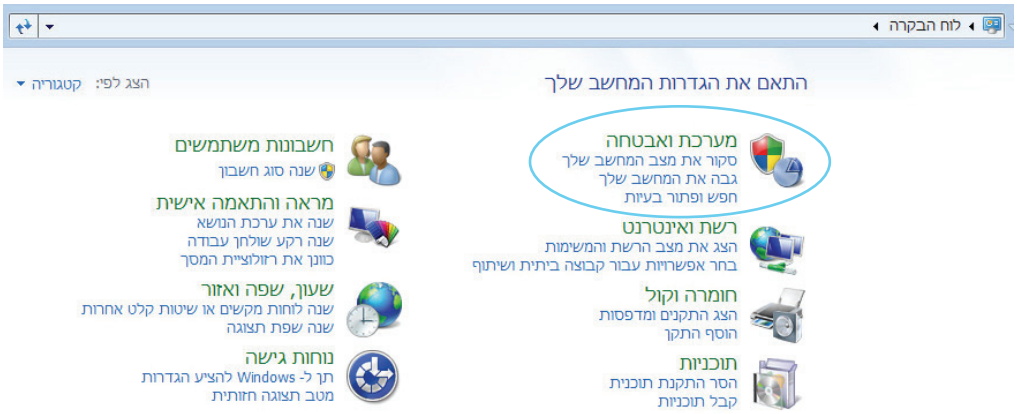
מחשבים וטלפונים ניידים מופעלים באמצעות תוכנת מערכת הפעלה ותוכנות שונות. ספקי התוכנה השונים מוציאים לשוק עדכוני תוכנה, לרבות עדכוני אבטחה, אשר נועדו לתקן כשל במערכות או פרצות אבטחה. עדכון התוכנות שברשותכם מטרתו למנוע את פרצות האבטחה המתגלות ובכך להקשות על תוקפים פוטנציאליים לתקוף.

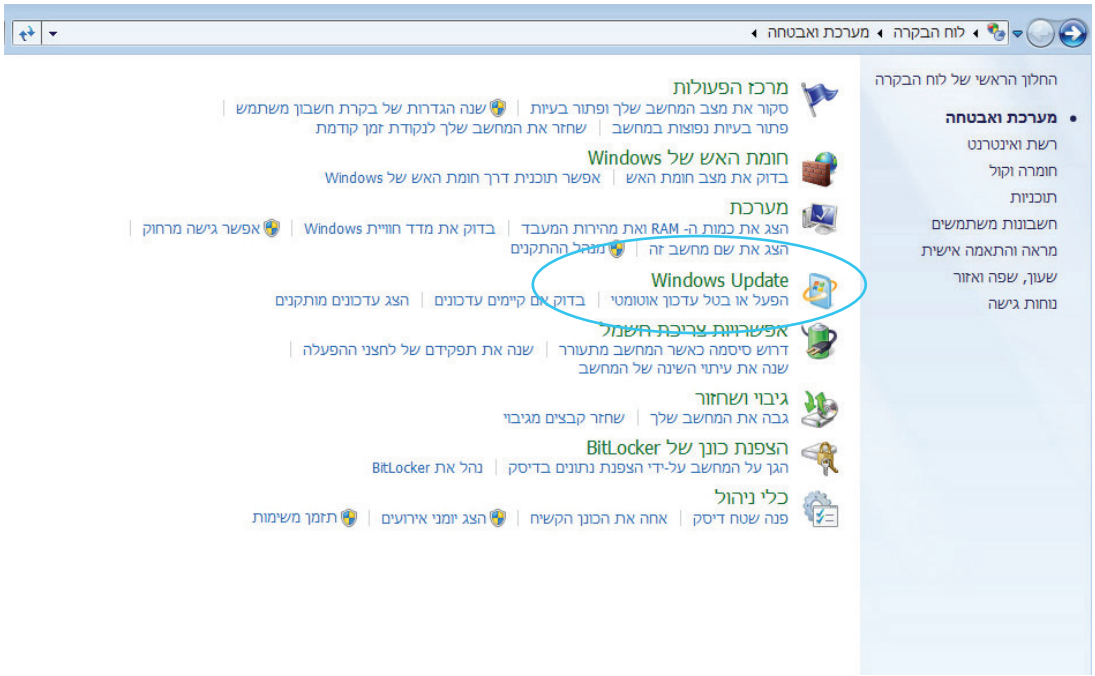
המלצות ודגשים

לוודא התקנת **תוכנות** Anti-Virus **וחומת אש** (Firewall) **ממקור מוסמך** (קיימים בשוק מוצרים רבים וטובים) בכל מכשיר שברשותך, תוך הגדרת קבלת עדכונים אוטומטיים וסריקה תכופה אוטומטית. הדבר נכון למחשבים, טלפונים חכמים ועוד.

להגדיר כי **עדכוני אבטחה למערכת ההפעלה** במחשב/במכשירך יופעלו באופן אוטומטי בעת פרסומם.

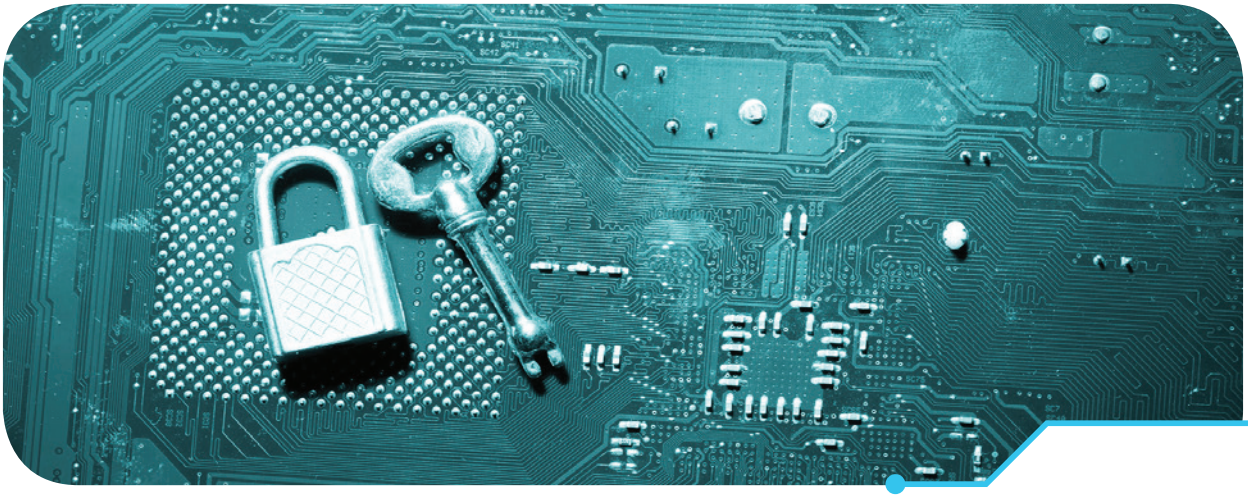
דוגמה להגדרת העדכונים, במחשב המופעל עם מערכת הפעלה Windows:





פרק 3

סיסמאות ובקרת גישה



הגדרת סיסמאות לשירותים השונים

סיסמאות הינן אמצעי קריטי באימות, ורצוי כי תהיינה קשות לניחוש. לפיכך מומלץ:

1. **הגדרת סיסמה בעלת אורך של לפחות 8 תווים, ומורכבת מאותיות גדולות וקטנות, מספרים וסימנים מיוחדים (!@#$)** - דבר זה יקשה על ניחושה.

2. **אי הישענות על פרטים מזהים** - יש לוודא שהסיסמה לא תרמז או תקשר לשם המשתמש שלך, לתפקידך או לפרטים מזהים אחרים כגון מספר ת"ז, תאריכי לידה, טלפונים ורמזים אשר ניתן למצוא בקלות ברשתות החברתיות.

3. **סיסמאות שונות** - הקפד שלא להשתמש בסיסמה אחידה או דומה לכל האפליקציות השונות שברשותך. שימוש בסיסמה זהה, משול ל"הנחת כל הביצים בסל אחד". כך, במקרה של פריצה לחשבון אחד שלך, התוקף יכול להשיג גישה לחשבונות אחרים שברשותך.

4. **שמירת הסיסמה באופן מאובטח** - אין לשמור במכשיר הסלולר, במחשב שלך או בפתק במשרד. ניתן לשנן, או להצפין את הסיסמאות הנבחרות.

5. **שחזור סיסמה** - אפליקציות/אתרים רבים מאפשרים לשחזר סיסמא שנשכחה, באמצעות מענה על שאלות מפתח, שהתשובה להן ניתנה על ידך בעבר. שים לב, כי בחרת שאלות שלא ניתן בקלות לדעת את התשובה שלהן. סקרים מראים, כי כ-50% מהתשובות לשאלות שחזור סיסמה באתרים שונים ניתנות לגילוי בקלות באמצעות איסוף מידע ברשתות החברתיות (שם הילד/ה, שם חיית מחמד, שם נעורים, בית

ספר וכו'). אפשרות נוספת היא לענות תשובה שאיננה אמיתית (למשל לענות תשובה מוצפנת) על שאלות "שחזור הסיסמה" באפליקציות השונות.

6. **הסיסמה הינה אישית** - מומלץ שלא להעביר את הסיסמה לחשבון שלך לאחרים. ברגע שהסיסמה ידועה ליותר מגורם אחד, לא ניתן לדעת או לעקוב אחר מי שביצע פעולה מסוימת בחשבון. בנוסף, הגדלת כמות האנשים שלהם העברת הסיסמה מגדילה את הסיכוי לחשיפתה.

7. **לקראת פעילות משמעותית (כגון יציאה להליך בחירות) חשוב להחליף את כל סיסמאות הגישה.**

8. **בשימוש ברשת Wifi ביתית**, חשוב **לשנות את סיסמת ברירת המחדל של נתב האינטרנט הביתי** לסיסמה פרטית. במידת הצורך, ניתן לפנות לספק האינטרנט לקבלת הדרכה.

אימות דו שלבי

באופן כללי, ישנם שלושה אלמנטים באמצעותם ניתן לזהות אותנו באופן חד ערכי: מידע **הידוע רק לנו** - כגון סיסמה, **אלמנט פיזי שנמצא בבעלותנו הבלעדית** - כגון תעודת זהות, ו**אלמנט בעל מאפיינים ביומטריים** - כגון טביעת אצבע.

דוגמה טובה כדי להבין את הנושא היא משיכת כסף מזומן מכספומט. לצורך כך, תידרש לשני אלמנטים של הזדהות: כרטיס האשראי שלך (אלמנט פיזי שבבעלותך הבלעדית) וקוד סודי (מידע הידוע רק לך). אם כרטיס האשראי שלך אבד או נגנב, אדם אחר לא יוכל להשתמש בו בכדי למשוך כסף מבלי לדעת את הקוד הסודי.

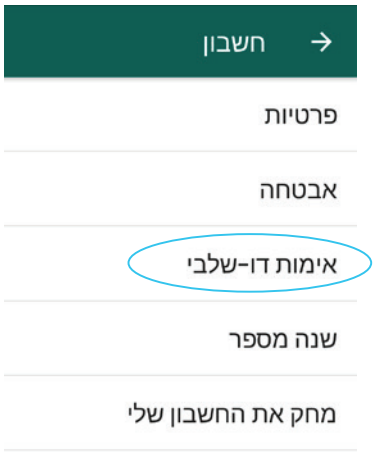
בכל אפליקציה משמעותית חשוב לבצע אימות דו שלבי - אימות דו שלבי מיועד להגן על המשתמש בכך שהוא מקשה על גורם עוין מלהיכנס לחשבונך. האימות משתמש בשני אלמנטים להזדהות: האחד, כניסה לחשבון באמצעות סיסמה (מידע הידוע רק לנו), השני - אמצעי נוסף ליצירת קשר כמו קוד המתקבל ע"י מסרון (באמצעות מכשיר הסלולרי שלנו, שהוא אלמנט פיזי הנמצא בבעלותנו הבלעדית), או קריאת טביעת אצבע (שהוא אלמנט בעל מאפיינים ביומטריים). בחירה באימות דו שלבי תקשה באופן מיטבי על הפורץ בפריצת הסיסמאות וכניסה לחשבונות.

מומלץ להגדיר "אימות דו שלבי" בדוא"ל (דוגמת GMAIL), במדיה חברתית ובאפליקציות השונות. במידה והתוקף הצליח להשיג את שם המשתמש והסיסמה - הגדרה זו תסייע לך להקשות עליו את תהליך ההתחברות לחשבון שלך. את ההגדרה של אימות דו שלבי ניתן לבצע בקלות דרך הגדרות ההגנה של התוכנות והאפליקציות.

להלן מידע נוסף על כיצד לבצע אימות דו שלבי במערכות ואפליקציות שונות:

חשבון/אפליקציה	קישור לאתר המנחה
Google (כולל דוא"ל)	https://www.google.com/landing/2step
Facebook	https://www.facebook.com/help/148233965247823?helpref=faq_content
Apple	https://support.apple.com/en-gb/HT204152
Microsoft	https://support.microsoft.com/en-gb/help/12408/microsoftaccount-about-two-step-verification
Twitter	https://support.twitter.com/articles/20170388
LinkedIn	https://www.linkedin.com/psettings/two-step-verification
Dropbox	https://www.dropbox.com/help/security/issues-two-step-verification
Instagram	https://help.instagram.com/1372599552763476

דוגמה לאימות דו שלבי:



הגדרת אימות דו שלבי ב-WhatsApp

הגדרת פרטיות

יש לבחון מעת לעת את הגדרות הפרטיות (הרשאות/ App permissions) של המכשיר הסלולרי והאפליקציות - לעיתים קרובות אנו מתבקשים לאשר חשיפת פרטים, אשר אינם אמורים להיות נחוצים. בדוק האם ברצונך לשתף את מיקומך הפיזי, לתת גישה לרשימת אנשי הקשר שלך וגישה ליומנך ליישומים להם ניתנו ההרשאות? במידה ואינך מעוניין, יש לבדוק שוב את ההרשאות שאושרו באפליקציות השונות, לשנות ולהקשיח את ההגדרות בהתאם.

האתר/אפליקציה	בחירת הגדרת הפרטיות / הסבר
Google	https://myaccount.google.com/privacycheckup
Apple	https://www.apple.com/privacy/manage-your-privacy
Facebook	https://www.facebook.com/help/443357099140264
LinkedIn	https://www.linkedin.com/psettings
Twitter	https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public
Instagram	https://help.instagram.com/116024195217477
Snapchat	https://support.snapchat.com/en-US/a/privacy-settings

פרק 4

הגנה על מחשב נייד ונייח

המחשב הנייח והנייד הינם כלי עבודה חשובים וככאלו, מידע רב מאוחסן בהם. פעמים רבות, הללו משמשים גם "שער כניסה" פוטנציאלי של תוקף לתוך הארגון. לפיכך הגנה על אמצעים אלו והמידע שבתוכם הינה בעלת חשיבות גבוהה מאוד.

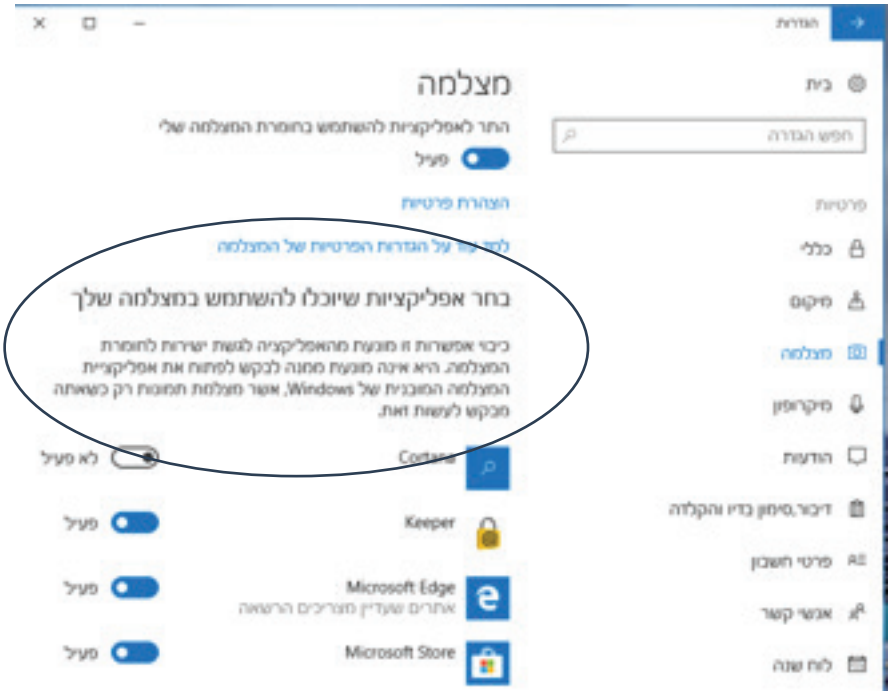
המלצות ודגשים:

יש לוודא כי בכל זמן בו לא מבוצע שימוש במחשב, הרי הוא **נעול** ולצורך פתיחתו נדרשת **סיסמה חזקה**. במידה ומתאפשר, רצוי להשתמש ב**אימות דו שלבי** (ע"ב טביעת אצבע או כרטיס חכם).

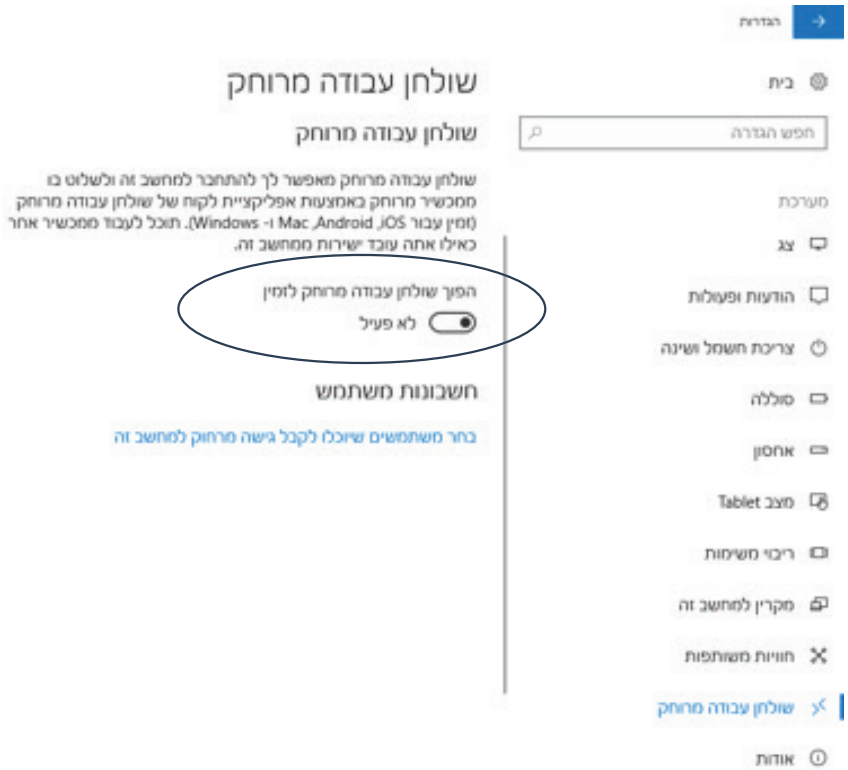
יש להימנע מלחבר התקנים חיצוניים ממקורות זרים/לא ברורים, למשל: Disk On Key, CD, התקני USB למיניהם, טלפון נייד של אדם זר. במידה ויש צורך להשתמש ב-DOK יש להשתמש באחד קבוע.

וודא כי התקנים כמו מצלמה או מיקרופון אינם מופעלים מרחוק - הסתר את המצלמה כל עוד אינה בשימוש, אשר שימוש רק לאפליקציות רלבנטיות.

דוגמה במחשב המופעל ע"י Windows:



4. יש להקפיד **לאשר השתלטות מרחוק** (למשל על המחשב) לצורך סיוע טכני **לגורמים מורשים בלבד** ורק לפרק זמן המוגדר למתן הטיפול בבעיה. מזער שימוש בתוכנות/כלי השתלטות מרחוק. לדוגמה במחשב המופעל ע"י Windows, הפוך את שולחן העבודה המרוחק ללא פעיל:



5. יש להקפיד **להתקין תוכנות רק מאתרים רשמיים ומוכרים**.

6. במידת האפשר מומלץ:
   - להימנע משימוש במשתמשים בעלי הרשאות גבוהות באמצעות צמצום כמות המשתמשים החברים בקבוצת Local Admin.
   - לבחון את ההרשאות הנדרשות בפועל ממשתמש Administrator. פעמים רבות, אופי השימוש של המשתמש אינו מצריך הרשאות מלאות.
   - לשנות את שמות המשתמשים guest, administrator.

7. **בטרם הוצאת המחשב הפרטי לתיקון, יש לבחון איזה מידע יהיה נגיש למי שיטפל במחשב?**

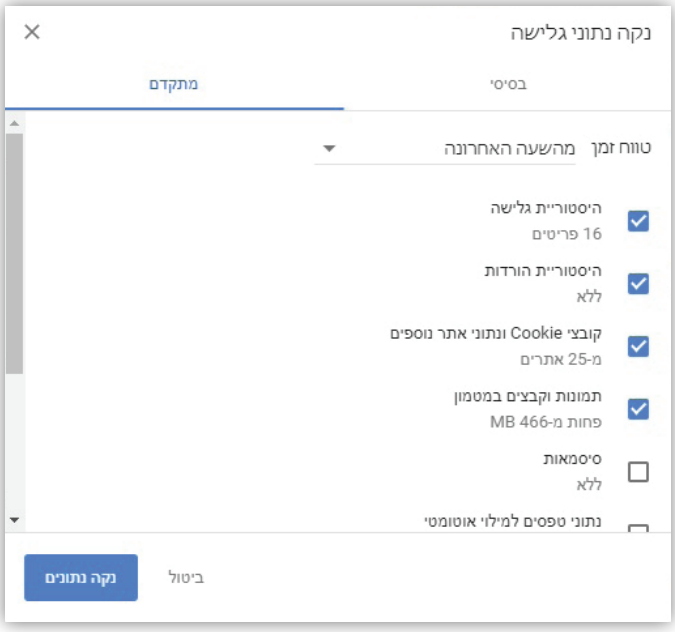
   - מומלץ **להימנע מלשים מידע רגיש על שולחן העבודה**.

   - לדאוג **לנעול באמצעות סיסמה קבצים רגישים**.

סוג קובץ	קישור להסבר כיצד להגדיר סיסמה לקובץ
PDF	https://helpx.adobe.com/il_he/acrobat/using/securing-pdfs-passwords.html
Office	https://support.office.com/he-il/article-הוספה-או-הסרה-של-הגנה-במסמך-cc3-300d-4c1a-8416-38d3e37d6826חוברת-עבודה-או-מצגת-05084/

   - **להתנתק (Log Out) משירותים חשובים** (כמו שירות דוא"ל או שימוש באתרים שונים) טרם מסירת המחשב.

   - יש לדאוג לבצע **מחיקת "עוגיות" (Cookies), קבצים זמניים והיסטוריית גלישה**. לדוגמה, בדפדפן מסוג chrome יש ללחוץ בו זמנית על Ctrl+Shift+Delete ולבצע ניקוי בהתאם:



פרק 5

הגנה על דואר אלקטרוני (Email)

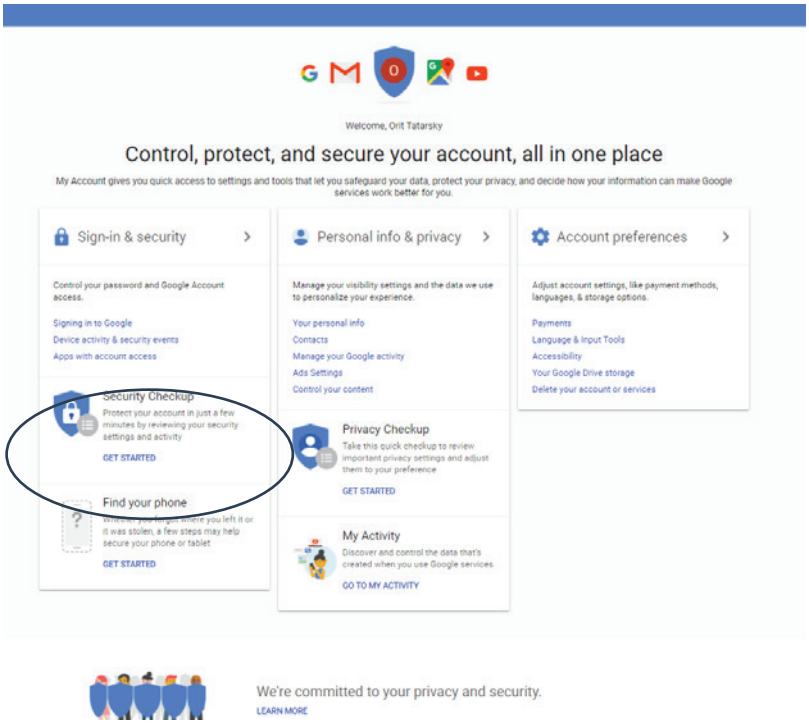
הדואר האלקטרוני הוא אמצעי תקשורת להעברת הודעות דרך רשת שרתים. הדוא"ל מהווה כלי עבודה משמעותי עבור כולנו. מידע רב, בחלקו רגיש מאוד, נמצא בשרתי הדואר האלקטרוני, חלקו מצוי בתוך הארגון אך חלקו מאוכסן בשירות חיצוני לארגון (למשל GMAIL ואחרים). בעזרת מספר הגדרות פשוטות ניתן להעלות את רמת האבטחה של הדואר האלקטרוני ולהקטין את הסיכוי שמישהו לא מורשה יוכל לקרוא את התכתובות שלך.

המלצות ודגשים:

לבחור ספק שרות דוא"ל מוכר, המספק שירותי דוא"ל מאובטחים.

עבור **תכתובות דוא"ל רגישות**, מומלץ שלא להיכנס אליהן בעת שימוש ב**רשת WIFI מזדמנת** (חינמית), כמו גם לא מרשת WIFI חיצונית אליה הנך נחשף באופן קבוע (למשל בית קפה בו הנך נוהג לשבת בקביעות). לתכתובות אלו עדיף להיכנס מהמחשב האישי ברשת מאובטחת או ממכשיר הסלולר הפרטי (על בסיס רשת הסלולר ולא ה Wi-Fi המזדמן/חיצוני).

להגדיר רמת אבטחה גבוהה בהגדרות האבטחה של הדוא"ל. לדוגמה, עבור gmail, ניתן להיכנס להגדרות חשבון google דרך: https://myaccount.google.com



חשוב להפריד חשבונות דוא"ל - במידה והנך בעל תפקיד ציבורי/עסקי, מומלץ לנהל חשבון אחד לדוא"ל שבו מתקבלות הודעות מהציבור הרחב (שמרביתן מתקבלות משולחים בלתי מוכרים), חשבון שני לדוא"ל בו נעשה שימוש פרטי וחשבון שלישי לדוא"ל לשימוש במסגרת תפקידך הציבורי.

קבלת התראות - בחשבון google ניתן להגדיר קבלת התראות בכל פעם שמתבצע ניסיון להיכנס לחשבון והסיסמה הייתה שגויה. במידה והיה ניסיון לפריצה והחשבון נחסם, ניתן תמיד לשחזר סיסמה. לשימוש בשירות יש להתקין את התוסף Password Alert ב-google chrome:
https://chrome.google.com/webstore/detail/password-alert/noondiphcddnnabmjcihcjfbhfklnnep?hl=en

בסיום כל התחברות לשירות הדוא"ל, יש לצאת באופן מסודר על ידי התנתקות. על ידי כך תוקף לא יוכל לנצל את החשבון המחובר בהיעדרך בהשתלטות עליו.

לא מומלץ להיכנס לחשבון הדוא"ל ממחשבים ציבוריים (כגון באינטרנט-קפה, ספריות ציבוריות, חדרי שירות עסקי במלונות וכו').

מודעות לפתיחת צרופות וקישורים:
במידה וקיבלת הודעה חשודה - אין למהר ללחוץ על קישורים או לפתוח צרופות, אפילו אם אינם חשודים. חשוב לבחון: האם הנך מצפה לקבל הודעה זו? מי השולח? והאם יש דרך להגיע למידע ללא לחיצה ישירה על הקישור? **האם ניתן לבצע הצגה מקדימה?**

ניתן לבדוק האם הקובץ נגוע באתרים שונים ע"י העלאת הקובץ לבדיקה (לדוגמה באתר https://www.virustotal.com). במקרה בו שולחים את הקובץ לבדיקה, יש לוודא שלא מדובר בקובץ בו המידע בעל רגישות גבוהה, בשל הסיכון בחשיפתו לגורמים זרים/עוינים.

■ **דוגמאות:**

- קישור המוביל לדף מתוך אתר אינטרנט, אשר עשוי להיראות אמיתי ורשמי - אך בפועל מדובר באתר מתחזה, באמצעותו מנסים לדלות את פרטי החשבון ע"י כך שהנתקף מתבקש להזין שם משתמש וסיסמה.

- דוא"ל ממשתמש בשם service@paypa1.com בו הנכם מתבקשים לבדוק חשבונית - בפועל, זהו דוא"ל המתחזה לדוא"ל לגיטימי מאתר PayPal והמשתמש בהטעיה ע"י שימוש בספרה 1 במקום באות l (הכתובת היתה אמורה להיות service@paypal.com).

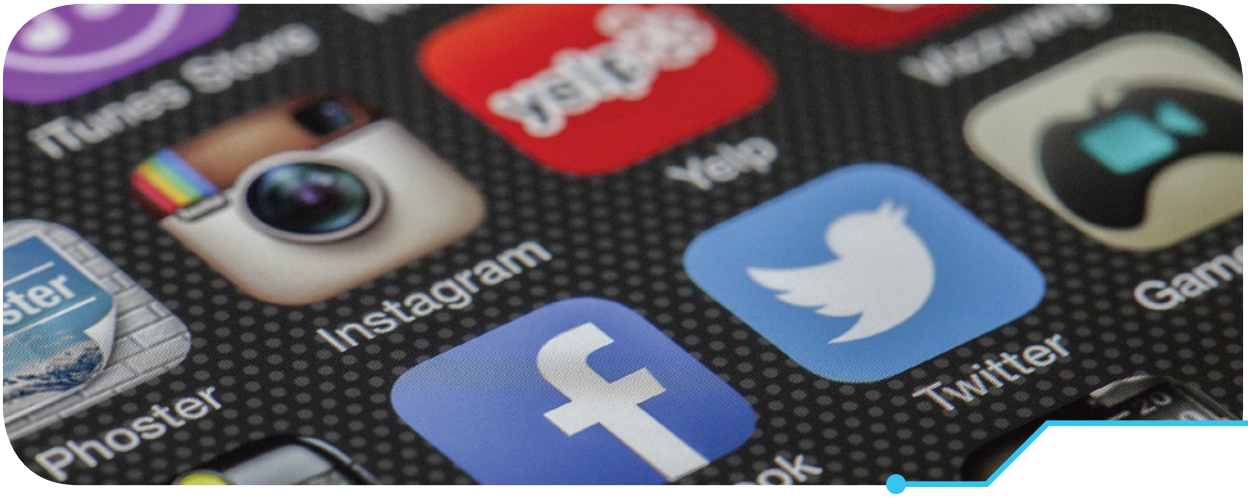
במידה וקיים חשד לגבי קישור, ניתן להעתיק את כתובת הקישור ולהדביק אותו בשורת הכתובת בדפדפן שבמחשב - בטרם לחיצה על Enter, יש לבחון את הקישור לעומק, לבדוק האם הכתובת מוכרת והאם אין בה משהו מעורר חשד.

במידה וכבר לחצת על הקישור או שפתחת את הצרופה - **ודא שלא מחקת את ההודעה** (על מנת שניתן יהיה לתחקר אותה) **ודווח מייד לאחראי המחשוב בארגונך.**

יישום DKIM/DMARC/SPF - למניעת הגדרות דואר כספאם, מומלץ להשתמש בפרוטוקולים מקובלים כגון DKIM, DMARK. ראה הרחבה טכנית להמלצה בקישור הבא:
https://www.gov.il/BlobFolder/reports/dmarc/he/DMARC-CERT-IL-W-350.pdf

פרק 6

הגנת פרופיל אישי ברשתות חברתיות



רשתות חברתיות (כמו Facebook, LinkedIn, Twiter, Instagram) מסייעות ביום יום לתקשר עם הבוחר, לפרסם אג'נדות, לעדכן ולשתף את הציבור בנעשה ועוד. אפליקציות אלו, מסייעות לקרב אותנו אל האחר באמצעות שיתוף תמונות, חוויות, פוסטים עם חדשות מעניינות ועוד. לצד היתרונות טמונות מספר סכנות אשר באמצעות מודעות ומספר צעדים פשוטים ומהירים - ניתן למזער אותן.

המלצות ודגשים:

חשיפה - יש לשים לב לפרטים - גורמים עוינים מסתובבים ברשתות החברתיות. שים לב לפרטים האישיים שאתה חושף לגביך ולגבי בני משפחתך. פרטים אלו מלמדים את התוקף על דפוסי ההתנהגות שלך, על הדברים שיעניינו אותך, ושבעזרתם יהיה קל לתקוף אותך - למשל לבצע עליך "הנדסה חברתית"[11].

כמו בדוא"ל גם כאן - **יש לנקוט משנה זהירות בלחיצה על צרופות וקישורים.** לדוגמה, לחיצה על מודעה המופיעה בפוסט ממקור לא ידוע עלולה להוביל לאתר מתחזה.

סיסמאות - בחר סיסמה קשה וארוכה, וודא אימות דו שלבי לכל חשבון רשת חברתית שברשותך[12].

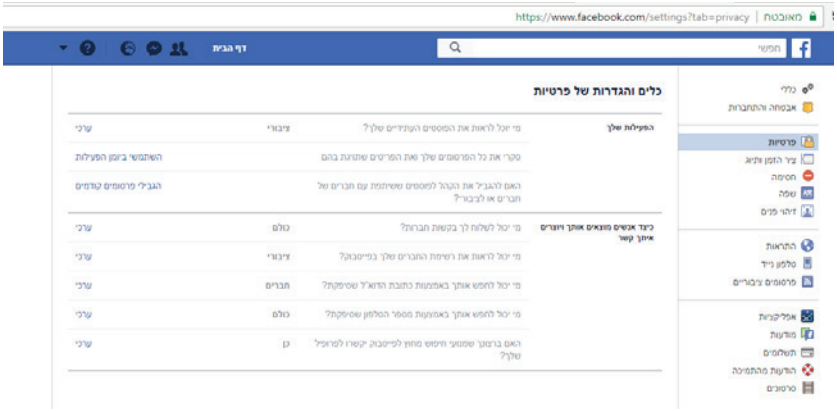
יש לבדוק את טפסי הרישום/הצטרפות/"צור קשר" בדף שלך (למשל בהגדרות דף ה-Facebook שלך) **ולצמצם המידע שאתה חושף** בהם למינימום ההכרחי. יש למחוק תוכן שדות אשר כוללים מידע רגיש ו/או מידע לא הכרחי.

---

11 ראה "הנדסה חברתית" בפרק 1.
12 ראה הסבר על אימות דו-שלבי בפרק 3.

רשימת עוקבים - שימו לב להגדרות המעקב אחריך. אילו נתונים יכול לראות מי שחבר שלך לעומת מי שעוקב אחריך? מהן הגדרות הפרטיות ושיתוף המידע שלך באפליקציות השונות?

דוגמה מ-Facebook:



היזהר מפרופילים מתחזים/מזויפים - פרופיל **מזויף** מציג אדם שאינו קיים ומשתמש בזהות בדויה, פרופיל **מתחזה** עושה שימוש בפרטיו של אדם אמיתי אחר, ומבצע פעולות ברשת תחת שמו של אותו האדם. התחזות היא עבירה פלילית.

פרופילים מסוג זה יכולים להיווצר גם באמצעות שימוש בטכנולוגיות אוטומציה ליצירת זהויות פיקטיביות, המאפשרות ליצור "רובוטים חברתיים" (Social bots) בכמויות גדולות. רובוטים אלה הם למעשה אלגוריתמים ממוחשבים שנועדו ליצור התחזות למשתמשי רשת אמיתיים, לרכוש ולנהל זהויות במדיה חברתית וכך לשמש כפלטפורמה להפצה מכוונת של תוכן תוך ניצול לרעה את כמותם ותפוצתם.

מאפיינים של פרופילים מסוג זה:

- **מיעוט מידע** - יכילו בדרך כלל רשימת חברים מצומצמת יחסית, מעט מאוד נתונים אישיים, מאגר דל של תמונות ו/או סרטונים, ציר הזמן או היסטורית הפעילות של המשתמש נראית ריקה בשנים קודמות, כלומר הפרופיל נפתח לאחרונה.
- **תמונת הפרופיל** נראית לעיתים מקצועית ובאיכות גבוהה מהרגיל.
- **תגובות** של פרופיל מסוג זה בשיחות פרטיות או קבוצתיות עשויה להכיל התבטאויות שאינן ראויות או קיצוניות, דברי הסתה, השמצה או אלימות.

מומלץ שלא לאשר חברות במקרה בו אין חברים משותפים.

פרק 7

הגנה על סמארטפונים ושעונים חכמים

הטלפון הסלולארי הפך מזמן לכלי מרכזי שלנו במרחב הסייבר, והוא שילוב של טלפון, מחשב, מצלמה, מכשיר הקלטה, מכשיר ניווט ועוד. בשנים האחרונות הצטרפו אליו הטאבלטים והשעונים החכמים. מה שמייחד את המכשירים הניידים הוא המגוון האדיר של אפליקציות שאנו יכולים לבחור להתקין עליהם, ואשר מאפשרות לנו להיות מקושרים ופרודוקטיביים יותר. אולם במקביל - אנו אוגרים בהם מידע רב ורגיש ומכשירים אלו צמודים אלינו לאורך כל היום.

מידע אופייני יכול לכלול: מיקומים (כמו מקום מגורים, עבודה, נוכחי, ועוד), אנשי קשר והיסטוריית שיחות, הודעות טקסט, קוליות ובתוך אפליקציות[13], היסטוריית גלישה וחיפוש, תמונות וקטעי וידאו ואודיו, דוא"ל רגיש, סיסמאות לחשבונות אישיים (כגון לבנק), נתונים בריאותיים ועוד. לכן, בראיית גורמים עוינים, זוהי פלטפורמה אידיאלית לביצוע תקיפה על המידע הרגיש שלנו.

המלצות ודגשים:

יש לוודא כי בכל זמן בו לא מבוצע שימוש במכשיר, הרי **הוא ננעל אוטומטית** ולצורך פתיחתו נדרשת **סיסמה/טביעת אצבע**.

מומלץ שלא "לפרוץ" את המכשיר - ישנן תוכנות ברשת המאפשרות לבצע זאת, אך לרוב הן גורמות להתקנת נוזקות על מכשירך ללא ידיעתך!

13 כגון Chat ב-Facebook.

יש להקפיד **להתקין תוכנות ואפליקציות רק מהאתרים הרשמיים**, המוכרים והמהימנים. תוקפים רבים מפיצים יישומים ניידים נגועים, הנראים לגיטימיים. התקנת אחד מיישומים אלו תקנה לתוקף שליטה מלאה על ההתקן הנייד שלך. מומלץ **להימנע מהתקנת אפליקציות חדשות** שזה עתה הועלו לחנות האפליקציות, שהינן בעלות מספר הורדות נמוך או שיש להם מעט מאוד משובים חיוביים מלקוחות. ככל שהאפליקציה בעלת וותק וזמינה, יותר אנשים ירשמו תגובות חיוביות וכן ניתן להניח כי האפליקציה אינה נגועה.

יש להקפיד להתקין **תוכנת Antivirus** מעודכנת.

יש להקפיד על **אימות דו-שלבי** לאפליקציות השונות שבשימושך[14].

יש לוודא כי **הרשאות הגישה של האפליקציות למאגרי המידע** (תמונות, קול, קבצים) **ולחיישנים** (מצלמה, מיקרופון, מיקום/GPS) הינן **ההכרחיות בלבד**. לדוגמה: אפליקציית פנס, שמטרתה להאיר, אינה אמורה להיות זקוקה לגישה לאנשי הקשר, לאלבום התמונות או למיקום הגאוגרפי (נ.צ) בו אתה נמצא. אם אתה מאפשר לאפליקציה תמיד לדעת את מיקומך, למעשה אתה עלול לאפשר למפיץ האפליקציה לעקוב אחר התנועות שלך ללא ידיעתך (ואף למכור מידע זה לאחרים). אם אינך מעונין להעניק את ההרשאות, יש לדחות את בקשת ההרשאות או לחפש אפליקציה אחרת שעונה לצורך שלך. מומלץ בעת התקנת האפליקציה מהחנות המורשית להסיר את הסימון (Checkbox) המאפשר לאפליקציה לקבל הרשאות מיותרות - ניתן לבצע זאת גם בדיעבד ע"י בחינת הגדרות הגישה בהגדרות המכשיר.

חנויות רשמיות להורדת אפליקציות:

חנות גוגל

https://play.google.com/store

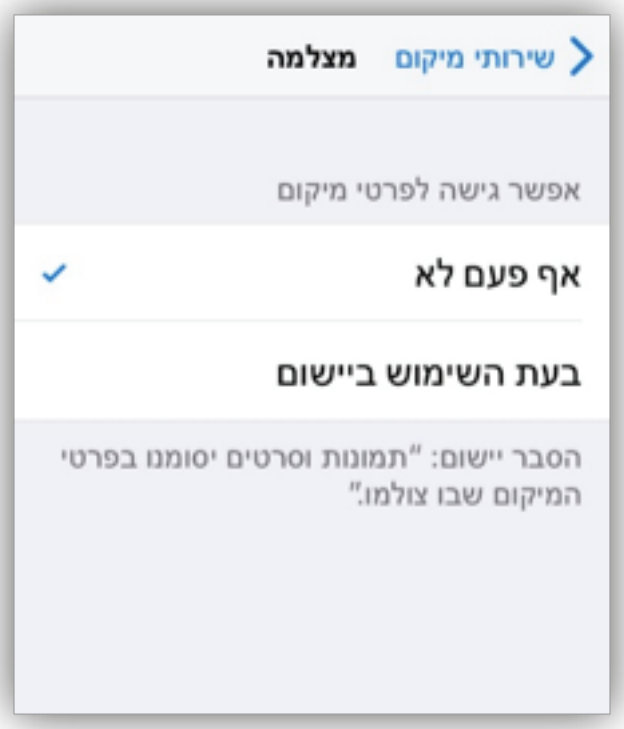
חנות iPhone

https://www.apple.com/ios/app-store/

14 ראה הסבר על אימות דו-שלבי בפרק 3.

בפרט רצוי **שלא לאפשר את התיוג האוטומטי של תמונות עם מיקום גיאוגרפי** (GPS) - כך תימנע ממקרים בהם העלית תמונה שצילמת לרשת חברתית, ותוקף פוטנציאלי יכול לאתר את מיקומך באמצעותה.

לדוגמה, ב-iphone, תחת הגדרות ← פרטיות ← שירותי מיקום:



יש להיזהר מהודעות SMS המגיעות ממספרים מוזרים בחו"ל - השיטה ידועה כאמצעי להנדסה חברתית; בוודאי שאין ללחוץ על קישורים וצרופות בהודעות אלו.

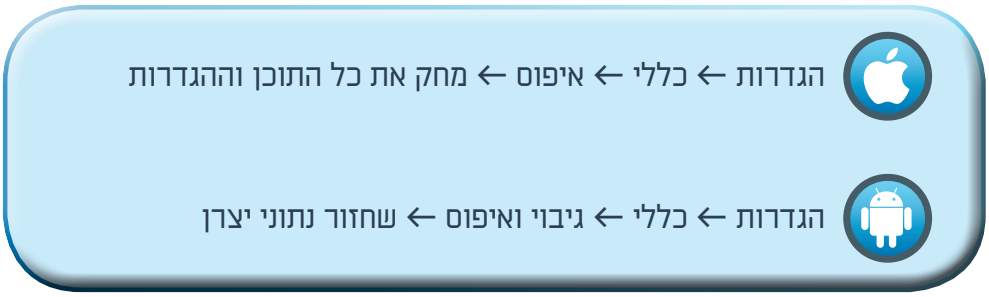
גם בסלולרי **אין לפתוח צרופות/קישורים המגיעים ממקור לא מוכר**, ייתכן מאוד שמדובר בניסיון דיוג[15]. במקרה וקבלת מייל או סמס חשוד, מומלץ לגשת באופן ישיר לאתר היעד, כלומר לא באמצעות הקישור שהתקבל **אלא באמצעות הקלדת הכתובת הראשית של האתר בדפדפן**.

יש לבצע **גיבוי עיתי** לכלל המידע - אנשי קשר, מידע אישי (קבצים, תמונות).

15 ראה הסבר על דיוג בפרק 1.

בעת **החלפת מכשיר** (למשל, לטובת שדרוג):

- חשוב **"לנקות" את המכשיר מכל מידע אישי. מחיקה פשוטה של הנתונים האישיים אינה מספיקה,** משום שניתן לשחזר בקלות את הנתונים. מומלץ לבצע **"איפוס להגדרות יצרן"**, פעולה אשר תחזיר את המכשיר למצבו המקורי בעת הרכישה:



- **גם לאחר ביצוע איפוס להגדרות יצרן במכשיר, מאוחסן בכרטיס ה-SIM מידע על חשבונות המשתמש.** לכן, במידה ולא ניתן להעביר את כרטיס ה-SIM (למשל כאשר הטלפון החדש משתמש בכרטיס SIM בגודל שונה) יש להשמיד פיזית/לגזור את כרטיס ה-SIM הישן בכדי למנוע מאדם אחר להשתמש בו.

- במכשירים ניידים רבים ניתן לבצע שימוש **בכרטיס SD** (Secure Digital), כרטיס זיכרון נפרד, לצורך הרחבת האחסון. כרטיסים אלו לרוב מכילים תמונות ותוכן רגיש אחר. חשוב לזכור להוציא את כל כרטיסי האחסון החיצוניים מהמכשיר הנייד. אם שימוש חוזר בכרטיס הזיכרון במכשיר החדש אינו אפשרי, אזי מומלץ להשמידו פיזית.

- במידה ונדרש למסור מכשירים לתיקון מומלץ להשתמש בשירותי **מעבדה מורשית** בלבד.

טיפ להגדרת Find my iPhone לאיתור מיקום נוכחי של מכשיר Apple -
https://support.apple.com/en-us/HT205362. בצורה פשוטה ניתן לגרום לנייד לצלצל, לשלוח לו הודעה, לנעול או למחוק נתונים מרחוק. שימושי כאשר המכשיר נגנב.

טיפ להגדרת איתור מיקום נוכחי של מכשיר אנדרואיד
https://support.google.com/accounts/answer/3265955?hl=en. ניתן מרחוק לגרום למכשיר לצלצל, לנעול אותו, למחוק פרטים. שימו לב שניתן לבצע את הפעולות כאשר המכשיר מחובר לרשת כלשהי. מכיון שגנבים נוטים לנתק את המכשיר מהרשת, מומלץ תמיד להצפין את המכשיר.

פרק 8

הגנה על אתר האינטרנט (Website)

הקמת אתר אינטרנט הינה פעולה הניתנת לביצוע כיום גם ללא ידע בתכנות ובאופן פשוט יחסית. ביצוע ההמלצות הבאות יתרמו רבות להגנה על זמינות האתר, אמינות המידע שיוצג בו והימנעות מפרסום מידע שחשיפתו עלולה לגרום לנזק. את הפעולות הבאות ניתן לבצע באופן עצמאי או שניתן לדרוש אותן מאיש המקצוע שבחרת.

- יש לבחון בעין ביקורתית את המידע שיפורסם באתר, בהתייחס לסיווגו הביטחוני, פגיעה בצנעת הפרט ו/או באינטרסים הפוליטיים שלך ושל הארגון שלך.
- במידה ובחרת להשתמש בספק שירות מקצועי לאתר, יש לוודא כי מדובר בחברה **מנוסה** בניהול, תחזוקה **והגנה על אתרי אינטרנט**.
- רצוי לבחור בכל **אפשרויות ותוספי האבטחה** שהספק ו/או יצרן פלטפורמת בניית האתר מציעים להגנה על האתר ולהקפיד על **הטמעת העדכונים** שהם מפרסמים.
- יש לדרוש שימוש בשרת או יישום **חומת אש אפליקטיבי** (WAF) כקו הגנה קדמי לסינון התעבורה מול האתר וחסימה לפי מזהים, חתימות ואנומליה, דבר אשר יסייע למניעת סוגי התקפה רבים. יישום כזה מוצע כיום כשירות על-ידי ספקים שונים בעלויות סבירות.

יש לדרוש מהספק **הקשחת הגישה לחשבון ניהול האתר** על ידי:

> סיסמה עם אימות דו-שלבי.
> שינוי ברירות המחדל של שם המשתמש וכתובת ה-URL של ממשק ניהול האתר.
> יש לקבוע מדיניות נעילת חשבון לאחר מספר כישלונות גישה.
> בעת בניית תשתית האתר יש להשתמש בחשבון **דוא"ל ייעודי**, נפרד ושונה מזה בו הנך משתמש בשגרה ו/או המפורסם באתר ליצירת קשר.

בבניית מסד נתונים (Database) לאתר, יש לדרוש מהספק לשנות בהגדרות את ברירת המחדל של **קידומת טבלאות מסד הנתונים** (Database table prefix), זאת על מנת להגן מפני תקיפת הזרקת קוד למסד הנתונים (SQL injection).

יש לרכוש ולהטמיע **תעודת הצפנה** לאתר (TLS/SSL) להגנה באמצעות הצפנת התעבורה בין דפדפני המשתמשים לשרת המאחסן את אתר האינטרנט, ע"י תעודה דיגיטלית מוכרת.

יש לקבוע **סיסמה מורכבת** למשתמשים ולניהול **מסד הנתונים** של אתר האינטרנט. מומלץ במידת האפשר לדרוש אימות דו-שלבי.

מומלץ לרכוש **שירות לגיבוי** האתר ומסד הנתונים שלו באופן שיאפשר התאוששות ועלייה לאוויר במינימום זמן.

יש להסיר את תיקיית ההתקנה של יישום בניית האתר במידה והנ"ל בוצע ממחשבך - כך תתגונן במידה ומחשבך ייתקף, מניצול תיקיית ההתקנה לפגיעה באתר.

טיפ לאנשי אבטחת המידע/אנשי ה-IT

לאחרונה אירעו מתקפות רבות בהן נמצא שימוש גובר בביצוע מתקפות בכלי המעטפת (Shell[16]).
שימוש זה יכול להתבטא בניצול חולשה בכלי המעטפת (למשל, חולשה בכלי PowerShell של חברת מיקרוסופט) או ניצול לרעה של תוקף ביכולת המעטפת.
בשל כך, מומלץ לעדכן את מערכת ההפעלה בטלאי האבטחה הרלוונטי אותו פרסם היצרן ולהגביל למינימום הנדרש את מספר העמדות מהן ניתן לבצע שימוש בכלי זה בארגון.
מידע נוסף והמלצות בנושא ניתן להרחיב בידיעה הבאה באתר מערך הסייבר הלאומי:
https://www.gov.il/he/Departments/publications/reports/campaignil

16 רכיב תוכנה המספק ממשק למשתמשים.

מערך ה-DNS

מהו DNS?

כתובת IP היא מספר חד-חד-ערכי המשמש לזיהוי נקודות קצה, כגון מחשב, ברשתות תקשורת שבהן משתמשים בפרוטוקול התקשורת IP, כגון רשת האינטרנט. לכל אתר אינטרנט ניתן לגשת באמצעות כתובת IP.

כיון שבני אדם זוכרים בקלות שמות, אך יתקשו בזכירת כתובות מספריות (דוגמת כתובות IP) הומצא ה-DNS (Domain Name System). ה-DNS מגשר על הפער הזה על ידי ביצוע המרה בין כתובת מילולית (המכונה URL), אותה זוכר המשתמש, לבין כתובת ה-IP בה בפועל משתמש המחשב על-מנת לתקשר עם היעד. URL לדוגמה יהיה www.cyber.gov.il.

שרת DNS הוא מעין ספר טלפונים ענק המאחסן את כל השמות ומאפשר את הצגתם באותיות ובמילים, במקום בכתובות IP.

מערך ה-DNS מהווה **תשתית חיונית** ברשת האינטרנט - ולפיכך מהווה **יעד להתקפות סייבר** מסוגים שונים - ביניהן התקפות מניעת שרות (DOS/DDOS), התחזויות והקמת אתרי דייג (phishing) במטרה להשתלט על אתרי אינטרנט ו/או לגנוב מידע אישי ועוד.

טיפים למנהלי אבטחת המידע/אנשי ה-IT

להלן מספר פעולות בסיסיות למזעור סיכונים למערך ה-DNS.

- **חיזוק השרידות**

ע"מ למזער את סיכון מניעת שרות ה-DNS חשוב לוודא שימוש בשני שרתי DNS לפחות.
בשורת cmd כותבים את הפקודה הבאה:
Nslookup –type=ns my_domain_name.org.il (דוגמה לשם מתחם)
בתוצאה של הפקודה צריכים להופיע לפחות שני שרתי DNS. לדוגמה:
my_domain_name.org.il namesever=ns1.my_domain_name.org.il
my_domain_name.org.il namesever=ns2.my_domain_name.org.il
בנוסף, לטובת השרידות, מומלץ להשתמש בשירותי שתי ספקיות DNS לפחות.

- **קבלת התרעות**

באופן כללי חשוב לזכור ששרתי ה-DNS הם חלק אינטגרלי וחשוב בתשתית המחשוב הארגונית שלכם (גם אם הם נמצאים באירוח במיקור חוץ), לכן יש לוודא שאתם מקבלים עליהם התרעות ניטוריות ואבטחתיות בצורה מסודרת.

- **מניעת התחזות לבעל דומיין ו"חטיפת" אתר**

ע"מ למנוע התחזויות של גורמים זדוניים לבעלי Domain מול ספקיות שרותי ה-DNS, חשוב לוודא שממשק העבודה מולן מוגן ע"י מנגנון אימות דו-שלבי.
חשוב לדרוש מספקיות ה-DNS שכל שינוי ב-Domain שלכם יחייב אישור פורמאלי ממנהל ה-Domain בארגונכם, שפרטיו שמורים מראש במאגרי המידע של ספקית ה-DNS.
ע"מ למנוע התחזות מול הרשמים (Registrars) חשוב לדרוש מהם לבצע פעולת lock על ה-Domain, וכך רק מנהל ה-Domain הארגוני יוכל לבצע שינויים. בנוסף, יש למסד מנגנון אימות דו-שלבי גם מול הרשמים.

- **DNSSEC**

DNSSEC (Domain Name System Security Extensions) הינו הרחבה אבטחתית של פרוטוקול ה-DNS, מטרתו להתמודד עם תופעות זדוניות שונות (ביניהן הפניית הגולשים לאתרים זדוניים וגניבת הפרטים שלהם) באמצעות בדיקת מהימנות ושלמות המידע העובר בתעבורת ה-DNS.
המלצתנו לכל בעלי ה-Domains אשר נמצאים באירוח בחברות hosting המספקות שרותי DNSSEC, לדרוש להפעיל שירות זה. לצורך כך יידרש מכם בנוסף לסכם את הנושא גם עם חברת הרשם (Registrar) המטפלת לכם ב-Domain.

- **שימוש בשם מתחם (domain) במרחב il.:**

מרחב שמות המתחם (domains) של מרחב IL. מנוהל על ידי איגוד האינטרנט הישראלי (ע"ר) תוך הקפדה על כללי אבטחת מידע גבוהים ובפיקוח מערך הסייבר הלאומי. מומלץ לבצע שימוש בשם מתחם במרחב IL. ולא בשמות מתחם במרחבים אחרים שאין ידיעה לגבי רמת ההגנה עליהם.

נכתב בשיתוף איגוד האינטרנט הישראלי (ע"ר) המנהל את מרחב IL. למידע נוסף עיינו ב-https://www.isoc.org.il/technologies-and-infrastructure-services/dns

פרק 9

גיבוי ויכולת התאוששות

פריצות עלולות להתרחש, למרות נקיטת אמצעי זהירות. במקרים רבים, כמו במקרה של כופרה, האפשרות היחידה לוודא שהמחשב אינו "מזוהם" בתוכנות זדוניות הינה "לפרמט" אותו - דהיינו, למחוק אותו לחלוטין ולהתקינו מחדש. במקרים אחרים אובדן מידע יכול להיגרם כתוצאה מתקלה או מחיקה בטעות.

במקרה מסוג זה, שחזור המידע מגיבוי יסייע להתאושש במהירות יחסית ולחזור לתפקוד. גיבוי הוא **עותק** של המידע הדיגיטלי שלך, **שאינו מאוחסן** על המחשב או ההתקן הנייד המגובה אלא **במיקום נפרד**, והוא מהווה "קו ההגנה" האחרון שלך!

המלצות ודגשים:

יש לבחון ולהחליט **מה לגבות** - ניתן לגבות רק נתונים חשובים או לגבות את כל המחשב, כולל את מערכת ההפעלה. בפתרונות גיבוי רבים (המוצעים ע"י היצרנים או ע"ב אפליקציות ייעודיות), מוגדר כברירת מחדל כי גיבוי הנתונים יבוצע עבור התיקיות הנפוצות ביותר בלבד - במידה וחשוב לך לגבות תיקיות נוספות, הגדר זאת במפורש. יש לוודא גיבוי למחשב נייח, מחשב נייד, מכשיר סלולרי וטאבלט.

יש לקבוע את **תדירות הגיבוי** - יש לוודא כי הגיבויים **יבוצעו באופן סדיר**. רוב פתרונות הגיבוי מאפשרים להגדיר לוח זמנים לגיבוי אוטומטי. חלק מהפתרונות מאפשרים גיבוי מיידי לקבצים חדשים/קבצים ששונו (בכל פעם שאתה שומר מסמך). אנו ממליצים על גיבוי אוטומטי יומי לכל הפחות.

יש לקבוע **היכן לגבות** - ניתן לגבות **להתקן אחסון נתיק** (כגון דיסק חיצוני נייד) או לגבות **לאחסון מבוסס ענן**.

•במידה ובחרת לגבות להתקן אחסון נתיק, מיד לאחר הגיבוי יש לנתקו ולשמור אותו במיקום נפרד ומאובטח, רצוי במקום מרוחק אשר יאפשר לך לבצע שחזור גם בעת שריפה או גניבה.

•גיבוי מבוסס ענן מבוצע באמצעות שירותים מקוונים המאחסנים את הקבצים שלך ע"ג האינטרנט. במקרה של גיבוי לענן, יש לוודא כי שירות הגיבוי מספק הצפנה של הנתונים ואימות דו-שלבי. בסיום ביצוע גיבוי לענן חשוב לזכור להתנתק מהשירות (לבצע logoff).

חשוב **לוודא יכולת שחזור** מהגיבוי.

מומלץ לבצע גיבויים במספר ערוצים במקביל (ענן / DOK / קלטות גיבוי וכד').

מומלץ לבצע גיבוי מקיף טרם מסירת מכשיר לתיקון.

במכשירי הנייד של Apple ניתן לבחור גיבוי ב-iTunes או iCloud. להסברים ניתן להיכנס לדף ההוראות: https://support.apple.com/en-us/HT203977

להסברים כיצד לגבות את חשבון Google ניתן להיכנס לדף:
https://support.google.com/nexus/answer/2819582?hl=en

פרק 10

התנהלות בטוחה

להתנהלות היומיומית בבית ובמשרד חשיבות רבה ביכולת להתגונן מפני סיכוני הסייבר. להלן המלצות בסיסיות להתנהלות בטוחה:

בחן מהו המידע הרגיש והחשוב ביותר שלך (ספריית התכתובות, בסיס נתונים של אזרחים, תמונות וכיוצ"ב) - הדלפה, שיבוש או מחיקה של מידע זה עלולים לגרום לך, לארגון שלך או למדינה נזק רב.

היה מודע לכך שהנך אחראי להגנה על המידע הרגיש שברשותך - בטלפון הסלולארי, במחשב הנייד, במחשב הנייח בבית ובמשרד, בחשבונות הדוא"ל, בחשבונות ברשתות החברתיות, באתר האינטרנט, במאגרי בוחרים שברשותך וכו'.

שמור על המכשירים הניידים שברשותך תחת השגחה (סלולארי, מחשב נייד, Disk on Key), הקפד לנעול את המשרד בו נמצא המחשב שלך.

תדרך את מורשי הגישה למידע שלך. וודא שהאנשים שיכולים לקרוא או לשנות את המידע שלך (עוזרים, בני משפחה וכו') מתודרכים בנוגע למה מותר ומה אסור ומודעים למובא במדריך זה.

בדיונים רגישים וודא עמידה בכללי ההגנה הנדרשים בהתאם לרגישות המידע. בפרט וודא כי אין בחדר אמצעי מחשוב בעלי יכולת האזנה/הקלטה - טלפונים סלולריים, שעונים חכמים, טלוויזיות חכמות וכד'.

היה בקיא ב**חוקים ותקנות רלוונטיים** - בפרט בתקנות 'חוק הגנת הפרטיות' המגדירות אחריות על שמירת מאגרי מידע המכילים נתונים אישיים של אזרחי ישראל.

בסיום שימוש נעל/צא מאפליקציות ומחשבונות - יש לוודא כי בכל זמן בו לא מבוצע שימוש במחשב הרי הוא **נעול**. בסיום שימוש באפליקציות ובחשבונות חשוב לבצע **יציאה מהחשבון** ("התנתקות"/Log out).

אל תשלח שמות משתמשים וסיסמאות בדוא"ל או בערוצים פומביים.

בשליחת דוא"ל לרשימת תפוצה, רצוי לכתב את הנמענים ב**עותק נסתר (BCC)** על מנת שכתובות הדוא"ל לא ייחשפו.

פרק 11

מה לעשות במידה והותקפת?

במידה והנך חושד כי הותקפת או מחשבך נפגע, יש לבצע את הפעולות הבאות:

1. **יש לדווח מיד על כל דבר חשוד. במקרה של חשד פנה לצוות אבטחת המידע/המחשוב במשרדך, או ל-CERT הלאומי בטלפון 9344*.**

2. במידה והנך חושד שקיבלת דואר מזויף, אין ללחוץ על הקישור/קובץ. דווח מיד לצוות אבטחת המידע/ המחשוב במשרדך ולנותן השרות.

3. גם במידה וכבר לחצת על הקישור או הצרופה החשודה, כאמור בסעיף הקודם, פנה מיד לצוות אבטחת המידע/המחשוב במשרדך - אל תמחק את הקובץ/צרופה על מנת שניתן יהיה לתחקר את מקור התקיפה.

4. יש לשנות מיד סיסמאות לכלל השירותים המקוונים. זאת על מנת למנוע מהתוקף קבלת הרשאות.

5. יש לבדוק באם מכשירים לא מוכרים התחברו לחשבונות שלך (בדרך כלל ניתן לראות זאת בעמודי הביטחון של חשבונך). במידה ויש לך אפשרות - יש לנתק מיד את כל המכשירים שאינכם מזהים.

6. במידה וטרם הגדרת 'אימות דו שלבי' על תיבת הדוא"ל וחשבונות המדיה השונים - מומלץ להחליף סיסמאות ולהגדיר אימות דו-שלבי.

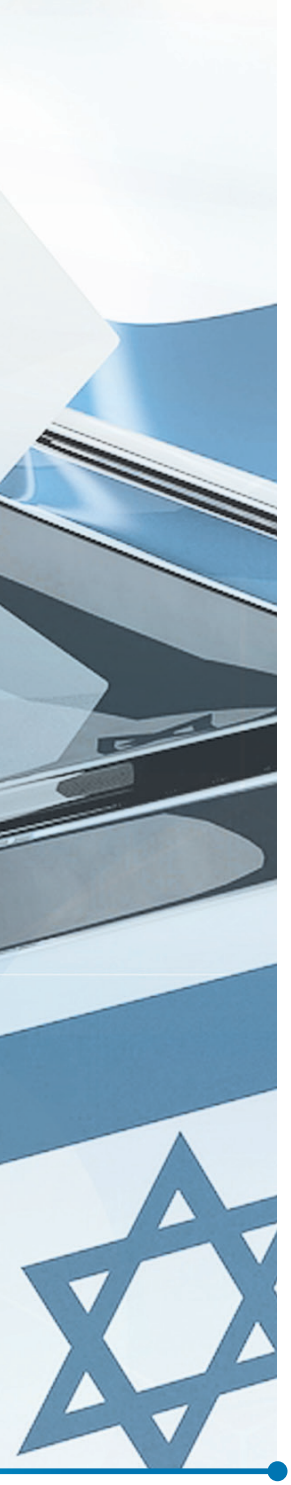
7. במידה והותקפת בכופרה - שים לב כי פעמים רבות, גם אם מועבר תשלום הכופר, אין התוקפים "משחררים" את ההצפנה. לסיוע ניתן להשתמש במדריך הנמצא ב:
https://www.nomoreransom.org/he/index.html

8. במידה ונפלת קורבן לעבירות הונאה, ואתה חושש כי נעשה שימוש בפרטיך האישיים לצורך מטרות פליליות, ניתן לפנות ליחידה הארצית לחקירות הונאה של משטרת ישראל או לפנות לתחנת המשטרה הקרובה למקום מגוריכם ולהגיש תלונה.

9. אם נחשפת למקרה של הטרדה אישית שהחלה ברשת אך יוצאת מגבולותיה ומהווה איום ממשי עבורך בעולם הפיזי, תוכל להגיש תלונה למשטרה או בקשה לבית המשפט לצו מניעה כנגד המטרידים, על פי חוק הטרדה מאיימת.

"עשרת הדיברות" להתנהלות בטוחה

1. **התייחסו לאבטחת הסייבר ברצינות!** ודאו כי המכשירים שלכם מקבלים עדכוני אבטחה באופן שוטף, וכי התקנתם אנטי וירוס
2. **יש להחליף סיסמאות** באופן שוטף. אין לבחור סיסמה אחת לכל החשבונות. בחרו בסיסמה ארוכה תוך שימוש באותיות, ספרות וסימנים (@#$%). הגדירו **אימות דו שלבי** לכל החשבונות החשובים, אחסון מיילים, מקורות אחסון המידע וחשבונות המדיה הדיגיטלית
3. בצעו **גיבויים תקופתיים** באופן סדיר
4. התקינו תוכנות ואפליקציות חוקיות ורק **מהאתרים הרשמיים**
5. לעולם **אין ללחוץ ולפתוח צרופות/קישורים** שהיו מצורפים לפניה חשודה - הקשיבו לתחושת הבטן!
6. **אל תתנו אישורים אוטומטיים** - בדקו היטב את הרשאות הגישה שאתם נותנים באפליקציות השונות (בדגש מיקום, מצלמה, מיקרופון)
7. **היו זהירים בפרטים אישיים** שאתם חושפים ברשתות החברתיות - הללו עלולים לשמש להנדסה חברתית
8. אל תחשפו מידע רגיש (כגון תכתובות דוא"ל רגישות, סיסמאות לחשבונות) **בעת גלישה ברשת** WiFi **לא מאובטחת**
9. ודאו **אבטחה נאותה לאתר האינטרנט** שלכם, בדגש DNS
10. בכל חשד לאירוע, **עדכנו את צוות אבטחת המידע/מחשוב** בארגונכם או פנו ל-CERT בטלפון 9344*



משרד ראש הממשלה
מערך הסייבר הלאומי

www.cyber.gov.il
CERT לאומי 9344*