סייבר ישראל
מערך הסייבר הלאומי

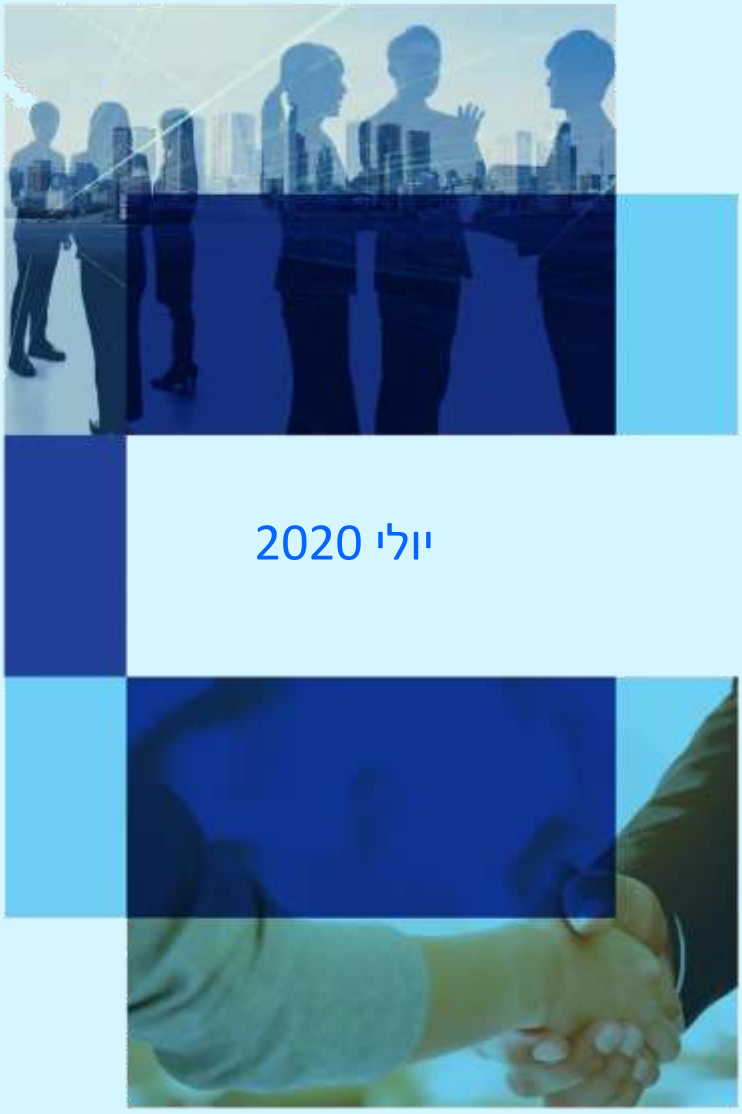
איומי סייבר ואבטחת מידע

חוברת הדרכה לעובד בארגון

סייבר ישראל
מערך הסייבר הלאומי

איומי סייבר ואבטחת מידע

חוברת הדרכה לעובד בארגון



יולי 2020

הדרכה זו נכתבה על ידי מערך הסייבר הלאומי לטובת הציבור ומשמשת כהמלצה לכלל הארגונים במשק הישראלי. ההדרכה ניתנת כשירות לעובדים בכל סוגי ההעסקה, וניתן לעשות בה שימוש חופשי לטובת שיפור רמת החוסן בסייבר במשק. כל הזכויות שמורות למערך הסייבר הלאומי. המלצות ההגנה יתעדכנו מעת לעת.

מומלץ שגורם מקצועי בארגון (מנהלי אבטחת המידע/CISO, מנמר"ים, גורמי משאבי אנוש, מנהלי ארגון, אנשי הדרכה בארגון) יעבירו את המצגת בפני העובדים, בהתאם לצורכי הארגון. ההדרכה כוללת מצגת וחוברת הדרכה, וכתובה בלשון זכר מטעמי נוחות בלבד. הערות והתייחסות למצגת ניתן להעביר בדוא"ל: ProfessionalTraining@cyber.gov.il.

תוכן עניינים

הקדמה

מדריך זה נכתב במטרה לחשוף בפני עובדים את הסיכונים שהם חשופים אליהם במרחב הסייבר, להעלותם למודעות ולסייע בקבלת כלים ואסטרטגיות להגנה בהיבט האישי, המקצועי והארגוני. המדריך מציג המלצות הגנה, שאפשר באמצעותן להבין את המשמעויות והסכנות הטמונות, זאת על מנת להקשות/להפחית ניסיונות תקיפה של גורמים עוינים במרחב האישי והארגוני. הכרת האיום חשובה וחיונית במטרה להקשות על התוקפים (ההאקרים) בביצוע מתקפת סייבר. חשוב לציין, שאין צורך להיות מומחה או בעל ידע טכני כלשהו, וכי על כל אחד ואחת מאיתנו מוטלת אחריות להקפיד על הנהלים כדי להגן על מרחב הסייבר (הזירה הדיגיטלית) ועל הארגון שבו אתם פועלים.

המדריך מקיף מגוון רחב של נושאים, וניתן כשירות לעובדים בכל סוגי ההעסקה, על מנת לאפשר למנהלי אבטחת המידע (CISO), מנמר"ים, גורמי משאבי אנוש, מנהלי ארגון ואנשי הדרכה בארגון להדריך את עובדיהם, בהתאם לצורכי הארגון, להגנה במרחב הסייבר.

מטרות-על:

1. הכרה והבנה של האיומים והסכנות הטמונות בפעילות במרחב הסייבר.
2. הכרת כלים בסיסיים לצמצום פגיעה עקב פעילות במרחב הסייבר האישי והארגוני.
3. הכרת הגורם המקצועי שניתן לפנות אלי ו/או לדווח לו במצב חירום.

הישגים נדרשים (מדידה והערכה):

העובד יכיר מונחים בסיסיים ממרחב הסייבר ואבטחת המידע.
העובד יכיר את הסכנות והחולשות הנפוצות במרחב הסייבר.
העובד יישם כלים להתמודדות ולהתגוננות בהיבטים אישיים וארגוניים.
העובד יידע כיצד להתנהל ו/או לדווח בעת אירוע חריג.

דרישות מוקדמות

אין צורך בידע קודם או ברקע טכנולוגי.
מומלץ שהדרכת העובד תכלול הסבר מקדים על מערכות הארגון, על תהליכים ושיטות עבודה, פעילותו, פריסתו ועל משימותיו. בהתאם לכך יפורטו הסיכונים והאיומים שהעובד עלול להיחשף אליהם ואופן ההתמודדות עמם.

אמצעי עזר

מצגת - ההדרכה תועבר לעובדים באמצעות מצגת מלווה, המשלבת סרטונים וקישורים ליצירת דינמיקה ואינטראקציה בין המרצה לעובדים. ניתן להוסיף אמצעים ושקפים נוספים הרלוונטיים לצורכי הארגון.
ערכת תוצרי מודעות - פרסומי מודעות ייעודיים בהתאם לנושאים הנלמדים (נספח א').

פרק זמן להדרכה

תכנון זמן ההדרכה ייעשה בהתאם לנושאים הרלוונטיים ולצורכי הארגון. לאורך ההדרכה חשוב ליידע את העובד מיהו הגורם המקצועי אשר יוכל להשיב לשאלות המתעוררות במהלך ההדרכה או בעקבותיה, לעודד את העובד לשאול ולחקור בכל עניין שאינו ברור ולעודד אותו לפנות לגורם האחראי.

אנו מקווים שהדרכה זו תסייע בהעמקת המודעות של עובדי הארגון לאבטחת מידע ותוביל להרגלי עבודה בטוחים יותר במרחב הסייבר של העובד והארגון.

מבוא - הבנת מרחב הסייבר

פרק זה מסביר מונחי סייבר בסיסיים להבנת מרחב הסייבר והכרת גורמי האיום. מטרת הפרק לסייע לעובד להכיר ולהבין את האיומים הקיימים, שעשויים להשפיע בהיבט האישי והארגוני.

מהו סייבר

מקור הביטוי "סייבר" הוא במילה האנגלית Cybernetics (או, בעברית - קיברנטיקה). כדי לקבל החלטות באופן יעיל ומועיל צריך מידע. על כן, הקיברנטיקה עוסקת רבות במידע על צורותיו השונות ובדרכים והשיטות שבהן הוא נוצר, מעובד, מוצג ומועבר ממקום למקום - זהו חיבור הקיברנטיקה למהפכת המידע, והביטוי המקוצר "סייבר" דבק במרחב החדש שבא לעולם. כיום מוגדר הסייבר כמרחב הכולל רשתות מחשבים ומערכות תקשורת.

מהו מרחב הסייבר

למרחבי היבשה, הים והאוויר המוכרים לכולנו הצטרף מרחב חדש, החוצה גבולות פיסיים, גיאוגרפיים, מדיניים ואחרים ומורכב ממחשבים רבים והתקנים אחרים (כמו מכשירי טלפון, מדפסות, בקרי ייצור תעשייתיים וכו'), ומשלל אמצעי תקשורת המחברים ביניהם (כולל רשתות קשר אלחוטיות). מרחב זה מכונה "מרחב הסייבר".
מרחב הסייבר הוא תולדה של קדמה טכנולוגית, קישוריות, מערכות מחשב וחיבור גלובלי לרשת האינטרנט. כיום אנו תלויים במחשבים בכל תחומי חיינו. מרבית השירותים והתשתיות שאנו נסמכים עליהם בהתנהלותנו היומיומית מנוהלים על ידי מחשבים ומכשירים חכמים.
מרחב הסייבר האישי מוכר לכולנו היטב: אתר אינטרנט אישי, דואר אלקטרוני פרטי ודואר אלקטרוני ארגוני, טלפון סלולרי, רשתות חברתיות - כל אלו הם כלים יומיומיים, המשמשים אותנו לטובת העבודה ומהווים חלק חשוב בשמירת קשרים מקצועיים, אישיים וחברתיים. לצד אלה מתפתח מרחב איומים, העלול להשפיע על רציפות התפקוד, האישית, הארגונית, שלמות תהליכי הייצור ועל סודיות המידע הארגוני.

מהי מתקפת סייבר

מתקפת סייבר הינה פעולה הננקטת על ידי גורם עוין, באמצעות מערכות ממוחשבות, על מנת לחדור ללא רשות למערכות המחשב של הקורבן במטרה לגרום נזק של גניבת מידע, פגיעה באמינות המידע ו/או בזמינותו (השפעה, תודעה, פיננסי, גניבת רכוש וכו').
השימוש הנרחב במערכות מחשב הופך אותן ליעד אטרקטיבי להתקפות, אשר להן עלולות להיות השלכות מרחיקות לכת עד כדי פגיעה בחיי אדם.

סוגי האיומים והגורמים במרחב הסייבר:

1. **הגורם האנושי (בשוגג או במזיד)**
גורם פנימי עשוי להיות:

- עובד הארגון
- עובד בעל הרשאות
- ספק שירות
- חולשות מובנות בתוכנה / חומרה / קושחה אשר הוטמעו על ידי הגורם האנושי - במזיד או בשוגג;
- קבלן/שותף עסקי שמצוי בקשר עסקי עם הארגון בהווה או בעבר. יש או היו לו הרשאות לרשת הארגון, למערכותיו או למידע האגור בהן (חריגה במכוון מהרשאותיו/ שימוש על מנת לבצע פעילות זדונית המונעת ממניעים פסיכולוגיים - כגון נקמה במעסיק, מניעים כלכליים - כגון גניבה או סחיטה על ידי גורמים חיצוניים, ומניעים אידיאולוגיים).

2. **ארגוני פשע ובעלי אינטרס כלכלי/אידיאולוגי**

3. גורמים בעלי אינטרס כלכלי, כגון מתחרה עסקי, ריגול תעשייתי וכד', או גורמים שיש להם מניעים אידיאולוגיים.

4. **האקרים (פצחנים)** - פועלים ממניע כלכלי או אפילו סקרנות של מתחילים, כמו סקריפט קידיס.

5. **האקטיביסטים** - בעלי מוטיבציה חברתית או פוליטית, אידיאולוגיה או אינטרסים שונים, כדוגמת אנונימוס (Anonymous), אשר פועלים מכל העולם נגד גורמים שנתפסים בעיניהם כפוגעים בחופש הביטוי

6. **מעצמות/מדינות זרות וגופי ביון**
מעצמות ו/או ארגונים עם יכולת כלכלית גבוהה ובעלי אינטרס לפגיעה בתודעה וביסודות דמוקרטיים, עם אפשרות להתערבות בבחירות, לתפיסת מעמד בשלטון, או יכולות צבאיות וכד'. כיום קיימות קבוצות תקיפה בחסות מדינות.

ערוצי הפצה לתוך הארגון

פרק זה מציג את ערוצי ההפצה הקיימים, שבאמצעותם תוקף יכול לנצל חולשות ופרצות כדי לחדור, למשל, לחשבונות אישיים או למערכות הארגון ולבצע נזקים משמעותיים.

תחנת קצה

אמצעי מחשוב או כל התקן שעובד משתמש בו בארגון, המחובר לרשת הארגונית ובאמצעותו ניתן לגשת לתוכנות, לאפליקציות ולמשאבי מידע ארגוניים ולצורך ביצוע תהליכים. ככזו, תחנת קצה חשופה למגוון איומי סייבר, הקשורים לשימוש העובד בעמדה, להגדרותיה ולקישורה לרשת הארגונית, והיא מהווה מטרה אטרקטיבית לתוקפים לשמש כשער לתקיפת הארגון. לכן יש חשיבות בהגנה על תחנות הקצה.

ההגנה תבוא לידי ביטוי באמצעות: אבטחה פיזית, הרשאות גישה, הצפנת מידע, תוכנות אבטחה, הגנה על ערוצי תקשורת והעלאת מודעות העובדים לחשיבות האבטחה. מידע נוסף והרחבה ניתן לקרוא באתר מערך הסייבר בפרק "המלצות הגנה לצמצום סיכוני סייבר בתחנות קצה בארגון".[1]

הגורם האנושי - התנהלות אישית

המשותף למרבית האיומים האפשריים על הארגון הוא הסתמכות התוקף על חולשות אנושיות של הקורבנות, לרבות עובד בארגון בעל סמכויות רבות. קיימת הסכמה רחבה בקרב מומחי אבטחת מידע, כי הגורם האנושי, יכול להוות חוליה חלשה בכל הקשור להגנת המידע והמערכות הממוחשבות בארגון. סקרים רבים אף מראים, כי קרוב ל-90% ממקרי דליפת מידע רגיש בארגונים מקורם בטעויות אנוש.

לרוב, התקיפה תתבצע על תחנה ברשת בעקבות התנהלות אישית (פתיחת קישור, הורדת קובץ, הכנסת DOK וכד').

תרחיש לניצול חולשה אנושית: תוקף יכול להתחזות לאיש תמיכה, המבקש מעובד הארגון שימסור לו את שם המשתמש והסיסמה שלו למערכת מסוימת (כספים, מש"א, מאגר נתונים וכד'). עם קבלת הפרטים, התוקף יוכל להיכנס למערכת ולהזדהות בשם העובד ולבצע פעולות זדוניות, כגון העברת כספים, איתור נתונים, שינוי פרטים וכיו"ב.

על כן, מודעות ל**התנהלות האישית** של עובדי הארגון, חיונית למניעת מתקפות במרחב הסייבר, ויש חשיבות גבוהה להעלאתה בקרב העובדים.

[1] המלצות הגנה לצמצום סיכוני סייבר בתחנות קצה בארגון:
https://www.gov.il/he/Departments/policies/endstation

כיצד מתרחשת מתקפת סייבר?

מתקפת סייבר מתרחשת לרוב בכמה שלבים מקדימים, שבהם התוקף נערך ומלקט כל מידע רלוונטי אשר יוכל לסייע לו בתקיפה, באם פרטנית או ארגונית. להלן השלבים:

1 איסוף מודיעין

התוקפים אוספים את מירב המידע על אודות הארגון, כולל מידע על בעלי תפקידים. איסוף המידע יכול להתבצע על ידי איתור מידע הקיים באינטרנט באופן פומבי, כמו רשתות חברתיות, מודעות גיוס, וכן על ידי איתור מידע מתוך הארגון, כדוגמת יומני פגישות, שיחות טלפון, מזכרים והודעות לעובדים, נהלים, רכש, ציוד מחשוב ישן, מידע ברשת האפלה או התגנבות לארגון לצורך מעקב וכד'.

2 חדירה ראשונית

לאחר איסוף המודיעין ובהתאם לנתונים הטכניים על עמדת הקצה יבחר התוקף את המטרה הנוחה או הפגיעה ביותר בארגון ואת שיטת התקיפה היעילה ביותר המתאימה לה, תוך שימוש בכלי התקיפה העומדים לרשותו (שליחת הודעה, מייל, נוזקה וכד'), זאת על מנת להשיג נגישות ראשונית לרכיב ממוחשב/לרשת הארגונית.

3 התבססות

עם הצלחת הפריצה הראשונית, תחנת הקצה המותקפת משמשת כשער כניסה לדילוג ולתקיפת שאר תחנות הקצה בארגון. לעתים התוקף יוריד כלי תקיפה נוספים אל התחנה המותקפת וישלים השתלטות עליה. לרוב, התוקף יפעל בחסות הרשאות של משתמש מורשה, שהשיג אותן במסגרת הפריצה הראשונית, ובכך יסווה את פעילותו ויקשה על איתור המתקפה.

4 התפשטות

לאחר ההתבססות בעמדת הקצה, התוקף משתמש בכלי תקיפה שהורדו אליה לצורך התפשטות לחלקים נוספים ברשת הארגון.

5 פגיעה

התוקף מנצל את ההשתלטות על הרשת הארגונית ומוציא לפועל של התקיפה לצורך גרימת נזק כלכלי, גניבת מידע ונתונים רגישים, פגיעה בקניין הרוחני, השחתת המערכות הקריטיות של הארגון או שיבוש הפעילות העסקית של המטרה המותקפת. לעתים, התוקף ידאג להשמדת כלי התקיפה ולמחיקת עקבות.

הידעת? לא כל מתקפות הסייבר פועלות בהכרח על פי שלבים אלו. לעתים התוקף ידלג על שלב זה או אחר, בהתאם למטרת התקיפה, הזמן והמשאבים העומדים לרשותו.

יש לציין, כי במקרים רבים, בעיקר במתקפות שמטרתן לגנוב מידע, הארגון לא יבחין כי היה יעד לתקיפה עד שיהיה מאוחר מדי, ולעתים אף לא יהיה מודע לכך לעולם.

סוגי נוזקות

לרוב, מתקפות סייבר מתבצעות באמצעות נוזקות - תוכנות מחשב זדוניות, שמטרתן לבצע פעולות לא לגיטימיות ברשת הארגון כמו לשבש פעולות מחשב, לאסוף מידע רגיש על המשתמש, לחדור ולהשיג גישה למערכות מחשב - כל זאת לצורך מימוש תקיפה ולרוב ללא ידיעת המשתמש.
ישנם סוגים שונים של נוזקות כאשר לכל אחת יש תפקיד בתהליך התקיפה. להלן דוגמאות לסוגי נוזקות:

- **רוגלה** - תוכנת ריגול, שמטרתה לאסוף מידע רגיש על אדם או על ארגון ללא ידיעתם, שעשויה לשלוח מידע זה לישות אחרת ללא הסכמת המשתמש, ו/או להשיג שליטה במכשיר ללא ידיעת המשתמש.

- **סוס טרויאני** - נוזקה המוחדרת להתקן קצה תוך התחזות לקובץ תמים במטרה ליצור דלת אחורית לרשת הארגון ולהדליף מידע אל מחוץ לארגון.

- **וירוס** - תוכנה החודרת למחשב באופן סמוי, משתמשת במשאבי המחשב להעתיק ולהפיץ את עצמה, ולרוב פוגעת בפעולה התקינה של המחשב הנגוע. לרוב, הווירוסים מוסווים כקבצים תמימים, אולם כאשר המשתמש פותח את הקובץ המצורף הוא מדביק את המערכת שלו בווירוס. וירוס עשוי להפיץ את עצמו למחשבים נוספים בדרכים שונות ובכך לשכפל ולהעצים את פגיעתו.

- **תולעת מחשב** - נוזקה המשכפלת את עצמה דרך הרשת ללא תלות בווירוס או בתוכנה נוספת ומפיצה את עצמה באופן עצמאי תוך שהיא מדביקה מחשבים אחרים. בניגוד לווירוס, שדורש הפעלה של קובץ או תוכנה נגועים, התולעת מפיצה את עצמה בצורה עצמאית על גבי רשתות פנימיות או רשת האינטרנט. דוגמה טיפוסית היא תולעת, שלאחר הדבקת המחשב שולחת את עצמה לכלל כתובות האי-מייל השמורות במחשב ומעמיסות על התקשורת ברשת. תופעות לוואי אפשריות של תולעת הן מחיקות קבצים ושליחת קבצים בדוא"ל מהמחשב הנגוע.

- **רישום הקשות (KeyLogger)** - חומרה או תוכנה, המאפשרת ניטור פעולות של המשתמש באמצעות הקלטת פעולות ואירועים של המקלדת, כגון סיסמאות, קודי גישה, תכתובות רגישות ועוד. הנוזקה תותקן על תחנת הקצה בעקבות לחיצה על הודעת פישינג המכילה קישור/צרופה, גלישה באתר זדוני או אתר שנפרץ, ניצול חולשה בדפדפן ועוד.

שיטות תקיפה נפוצות

עובדי הארגון יכולים לשמש קורבן למתקפת סייבר. פרק זה יציג מונחים ושיטות תקיפה נפוצות שחשוב להכיר. העלאת מודעות העובד לשיטות התקיפה השונות, בליווי דוגמאות רלוונטיות לארגון או היבטים אישיים יסייעו בתהליך ההבנה וההתמודדות עם ניסיונות התקיפה.

הנדסה חברתית

ביצוע מניפולציה וניצול תכונות פסיכולוגיות אנושיות על מנת לגרום לאדם לציית לבקשותיו של גורם עוין שמעוניין בגישה למערכות הארגון, למידע פרטי וכו'. באמצעות הונאה ומניפולציה התוקף משכנע את הקורבן - ללא ידיעתו - לבצע פעולה אשר עלולה לחשוף מידע רגיש, תוך שהוא עוקף את מנגנוני האבטחה. באמצעות הנדסה חברתית הנתקף עלול, ללא ידיעתו, לאפשר לגורם עוין גישה למערכות הארגון, גישה למידע פרטי (כמו מסירת פרטי התחברות), וגרימת נזק משמעותי.

במתקפה המתבססת על הנדסה חברתית ינצל התוקף חולשות אנושיות כדוגמת סקרנות, פחד, הטעיה או פיתוח ציפיות במטרה לגרום לקורבן לבצע את הפעולה המבוקשת. לרוב, התוקף יתמקד בגורמים בארגון, שיש להם גישה למידע או למשאבים שבהם הוא מעוניין (זוטרים ועד בכירים). תרחישים אפשריים למתקפות שכאלו הם:

- ❑ שליחת הודעת דוא"ל בהולה למנהל הכספים, כביכול בשם המנכ"ל, המבקש לבצע העברת כספים דחופה לחשבון חסוי.
- ❑ שליחת קובץ זדוני, המתחזה לקובץ משכורות לידי עובדים שונים בארגון.
- ❑ לחיצה על קישור תמים למראה, המוביל אל אתר אינטרנט אשר מושתל בו קוד זדוני. כאשר לוחצים עליו - הוא פוגע ומדביק את המכשיר של המשתמש.
- ❑ הורדה של קובץ (מסמך, סרטון, תוכנה וכו') המכיל וירוס המדביק את המחשב.
- ❑ מסירת מידע רגיש לגורם עוין, המתחזה לאדם לגיטימי (לקוח, מנהל בכיר וכו').

דיוג (Phishing)

שיטה זו היא הנפוצה ביותר מבין שיטות התקיפה של הנדסה חברתית. **התוקף פונה לתפוצה רחבה של אנשים** (בדומה להטלת רשת דיג) ומנסה "להעלות ברשתו" מידע אישי רגיש או פיננסי של המשתמש, כאשר הקורבן מוסר בעצמו, שלא במודע, את המידע לתוקף. בשיטה זו התוקף מייצר, למשל, אתר מזויף, הודעת דואר אלקטרוני (דואר זבל/ספאם), מסרון (SMS), שהקורבן מגיב להם במחשבה כי הם אמינים. כאשר הקורבן מזין את פרטיו האישיים (מספר כרטיס אשראי, סיסמאות לחשבונות וכדומה) באתרים מזויפים אלו, הוא למעשה מוסר את המידע שלו לתוקפים, אשר יכולים לעשות בו שימוש תוך התחזות לקורבן.

דיוג ממוקד (Spear Phishing)

שליחת הודעה ממוקדת **לאדם ספציפי או לקבוצה ממוקדת**. בניגוד להתקפת דיוג, המבוצעת כאשר התוקף פונה לתפוצה רחבה של אנשים, דיוג ממוקד מותאם אישית למספר קטן מאוד ונבחר של אנשים, לאחר שהתוקף אוסף עליהם מידע ואף לעתים מצליח לחדור למערכות הארגון. פנייה מניפולטיבית לנתקף תהיה לרוב סבירה ושגרתית וקשה לזיהוי. לעתים קרובות היא תגיע מכתובת שתיראה כמו כתובת של גורם מוכר או עמית, ולפעמים היא אף עשויה להיראות כמענה לתכתובת אמיתית שניהל המקבל עם שולח ההודעה. במקרים רבים פניות אלו מנוסחות בצורה שיוצרת תחושה של דחיפות ובהילות, הדוחפות את הקורבן לנקוט פעולה מיידית בלי בדיקה וללא התייעצות.

ווייל פישינג (Whale Phishing)

סוג של הונאה ממוקדת ולרוב מתוחכמת מאוד, המופעלת על גורמים מפורסמים או על בכירים בארגון.

סמישינג (SMS Phishing)

דיוג באמצעות הודעות SMS או WhatsApp, כאשר התוקף עשוי לשלוח הודעות בתוספת קישור זדוני לכתובת או להורדת קובץ/תמונה/סרטון.

וישינג (Voice Phishing)

הונאת הנדסה חברתית, הנעשית באמצעות שיחות טלפון שבה התוקף מתחזה לגורם לגיטימי ומבקש מהמותקף לחשוף פרטים אישיים, פיננסיים או לבצע פעולות במסווה תמים.

דוגמאות להונאות דיוג (Phishing):

- ❑ קבלת דוא"ל מזויף, שנראה כאילו נשלח מצוות התמיכה, המבקש להיכנס לקישור זדוני ולהזין בו את שם המשתמש והסיסמה.
- ❑ קבלת דוא"ל מזויף, שנראה כאילו נשלח מחברה לגיטימית (למשל: פיי-פאל, אמזון, חברת אשראי, בנק וכו'), המבקש להיכנס לקישור זדוני ולהזין בו את שם המשתמש והסיסמה. לעתים המשתמש אף יתבקש להזין פרטים נוספים, לכאורה לצורך אימות נוסף ו"בטוח", כדוגמת פרטי אשראי, מספר טלפון, כתובת מגורים, שאלות אבטחה ועוד.
- ❑ פרסומת באתר אינטרנט, המציגה הצעה שיווקית אטרקטיבית (לרוב מפוקפקת), המובילה לאתר זדוני.
- ❑ הודעת אזהרת אבטחה, המתריעה לכאורה על פריצת אבטחה ומציעה לנתקף להחליף סיסמה בקישור שנשלח.
- ❑ קבלת הודעת טקסט ("סמישינג") - באמצעות הודעת SMS או WhatsApp עם קישור לאתר או להורדת אפליקציה זדונית.

הידעת? לא תמיד קל לזהות הודעת דיוג. כל אחד עלול ליפול כקורבן להודעת פישינג ויכול בתום לב ללחוץ על קישור או לפתוח צרופה. חשוב מאוד שבמידה וזה נעשה, אל תפחדו או תתביישו, דווחו מיד לגורם האחראי בארגון, זאת על מנת לצמצם את הנזק האפשרי.

שקף 12 מציג דוגמאות לניסיונות דיוג שונים אשר נשלחו במדיות השונות.

כופרה (Ransomware)

מתקפת כופרה מתבצעת על ידי התקנת תוכנת כופר זדונית, המצפינה את הקבצים המאוחסנים במחשב ומונעת כל גישה למערכות המחשב ולמידע, תוך הצגת דרישת תשלום כופר למפעיל הנוזקה. הכופרה בדרך כלל מצורפת לקובץ בדואר האלקטרוני/קישור בהודעת טקסט/קישור באתר אינטרנט, כאשר ברגע שהנמען פותח את הקובץ/קישור, מותקנת הכופרה ומפעילה את הצפנת הקבצים. עם השלמת הפעולה תופיע הודעה, המבשרת למשתמש כי קבציו הוצפנו, וכי עליו לשלם עבור שחרורם באמצעות מערכת תשלומים שלא ניתנת למעקב (כגון העברה בנקאית, שימוש במטבע וירטואלי Bitcoin ועוד).

התרשים בשקף מציג את שלבי התקיפה של מתקפת כופרה.

ניתן להציג את התהליך עם דוגמאות רלוונטיות לארגון.

יצוין, כי לעתים קרובות גם תשלום הכופר לא בהכרח יוביל את התוקף לשחרר את ההצפנה.

ניתן להציג את אתר No More Ransom, אשר הוקם על ידי רשויות אכיפת חוק וחברות אבטחת מידע (משטרת הולנד, יורופול וחברת McAfee), בשיתוף עם משטרת ישראל, במטרה לסכל את פעילותם של עברייני סייבר המעורבים בהפצת תוכנות כופרה, ולסייע לקורבנות תוכנות כופרה בפענוח הקבצים שהוצפנו מבלי לשלם לפושעים. האתר מתורגם לשפות רבות, **כולל עברית**.

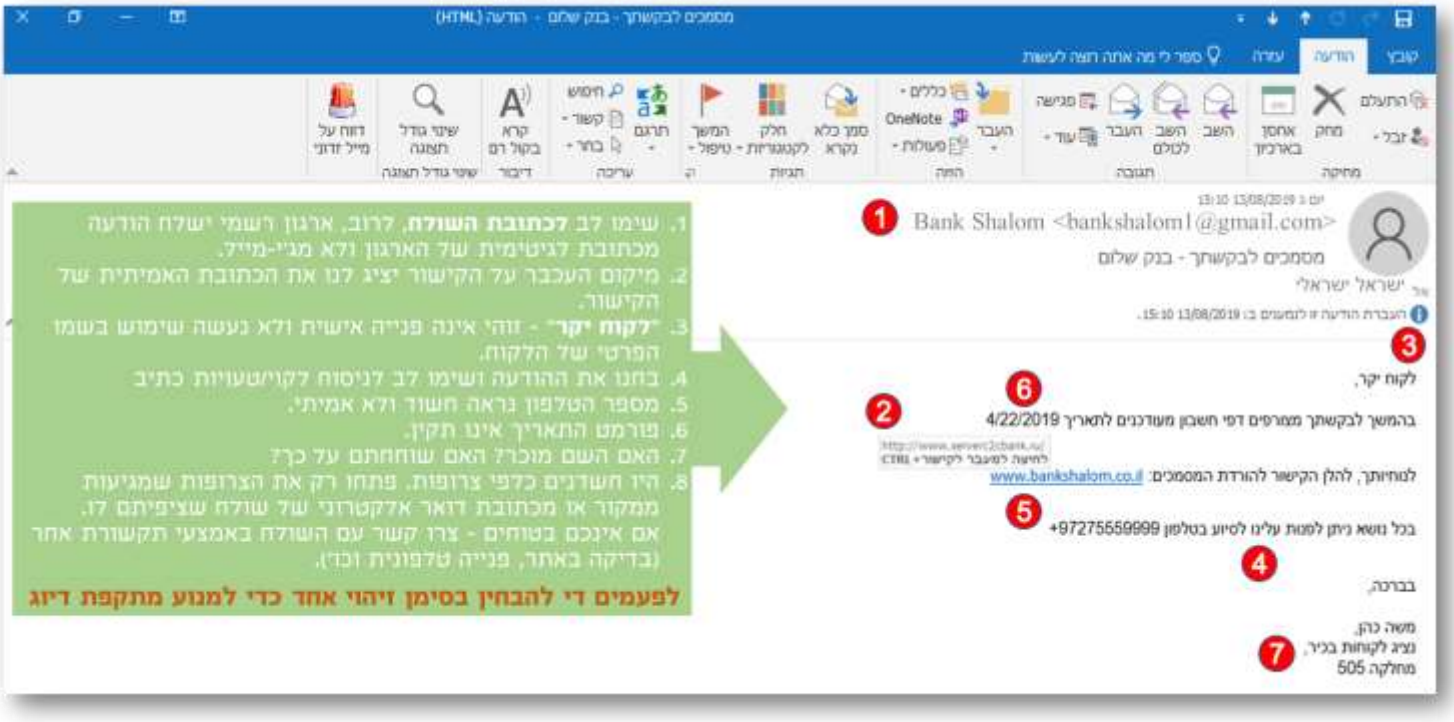
קישור לאתר: https://www.nomoreransom.org/he/index.html

המלצות בסיסיות להתגוננות

פרק זה מציג את הכלים הבסיסיים, אשר בעזרת ערנות ומודעות יוכלו לסייע לכל אחד ואחת בארגון להתגונן, להקשות על תוקף לפגוע במערכות מחשוב של העובדים בהיבט האישי והארגוני. הכרת הכלים הבאים והטמעתם תקשה על התוקף לפגוע במרחב הסייבר האישי והארגוני.

מניעת דיוג (Phishing)

השקף הבא מציג דוגמה לדוא"ל דיוג חשוד. ניתן להציג לעובדים את כלל הדוגמאות והנושאים שחשוב להתייחס אליהם בעת קבלת דוא"ל מגורם זר ואפילו מגורם מוכר. ניתן גם לייצר דוגמה לדוא"ל עם הנושאים הרלוונטיים.



הגדרה וטיפול בסיסמאות

הסיסמה משמשת אמצעי זיהוי אישי לשם בקרת גישה לחשבונות השונים. אנו נדרשים ליצור סיסמת זיהוי בכל תוכנה/אפליקציה שבה אנו עושים שימוש. תוקף אשר משיג סיסמה לחשבון יכול לקבל שליטה על הנכסים האישיים כמו חשבונות, פרטי בנק, כניסה למחשב ועוד. בבחירת סיסמאות יש להתייחס לסעיפים הבאים:

- חשוב לבחור סיסמה ארוכה ומורכבת, המכילה אותיות גדולות וקטנות, ספרות ותווים מיוחדים (@#$!). מומלץ להרכיב משפט ארוך הידוע רק לנו (לדוגמה: iLoveIceCream@21)
- אין לכלול פרטים אישיים, אשר ניתן לאתר בקלות ברשתות החברתיות (ת"ז, מספר טלפון, שמות ילדים וכד').
- הסיסמה היא אישית - אין לשתף סיסמאות עם אף אחד!
- יש לבחור סיסמאות שונות לחשבונות ולמכשירים שונים, וזאת על מנת למנוע מצב שבו חשיפת סיסמה לחשבון מסוים תאפשר גישה לכלל החשבונות שלכם.
- אין לשמור את הסיסמאות במכשיר הסלולרי או במחשב, ואין לרשום את הסיסמה בפתקים או במקומות נגישים. יש לשנן או להצפין את הסיסמאות.
- חשוב להגדיר אימות דו-שלבי לכל חשבון המאפשר זאת.
- ניתן גם להשתמש בתוכנה/אפליקציה לניהול סיסמאות, המאפשרת לשמור את כל הסיסמאות לחשבונות השונים כאשר יש צורך לזכור רק סיסמה אחת.

אימות דו-שלבי (2FA) / רב-גורמי (MFA)

זהו אמצעי להוספת שכבה נוספת של אבטחה לחשבון משתמש במטרה למנוע מצב של גניבת חשבון, הונאה או גניבת זהות ויוצר צורך לאמת את הזהות של המשתמש ב**שני שלבים**:

זיהוי - המשתמש טוען מהי זהותו (שם משתמש, מספר חשבון, מספר תעודת זהות, כתובת מייל וכו').
אימות - המשתמש מגבה את זהותו באמצעות הצגת שני מזהים מבין האפשרויות האלה:

- **מידע הידוע רק למשתמש** (Something you know) - כגון סיסמה, PIN, שאלת אימות.
- **מידע לגבי המשתמש עצמו** (Something you are) אמצעי פיזי, כמו טביעת אצבע, זיהוי קול/פנים/קשתית.
- **מידע האגור במכשיר הנמצא ברשותו של המשתמש** (Something you have) - מחשב, טלפון נייד, כרטיס RFID, כרטיס חכם, USB TOKEN וכד'.

קיים מונח נוסף, שנקרא **אימות רב-גורמי** (MFA), והכוונה לאימות באמצעות שימוש בשני גורמים או יותר.
מרבית התוכנות המוכרות והרשתות החברתיות המובילות מאפשרות כיום לבצע אימות דו-שלבי, וניתן להגדירו בקלות בהגדרות ההגנה/האבטחה של האפליקציות השונות.

הגנה על מכשירים במשרד

לעתים אנשים מקלים ראש בשמירה על כללי אבטחת המידע. חשוב להעלות את המודעות לשמירה על הכללים בעת עבודה במשרד.

התנתקות ונעילת מחשב - בכל יציאה מהמשרד או בסיום יום העבודה חשוב לבצע התנתקות מסודרת מהחשבונות, ונעילה של המחשב. ניתן לבצע זאת על ידי לחיצה מקוצרת: *Ctrl+Alt+Delete* - נעל. בסיום יום עבודה יש לכבות את המחשב.
כאשר עובדים עם מחשב נייד - יש לנעול אותו באמצעות סיסמה, קוד, נעילת דפוס, אמצעי ביומטרי.
גיבויים - יש לוודא בארגון אכן מתבצעים גיבויים עתיים במחשב ובמכשירים הניידים שברשות העובדים. כמו כן, יש לוודא את תקינות הגיבויים וכן שמירה עתית של הגיבויים באופן לא מקוון (ניתן לגבות בכונן חיצוני למחשב - שאינו מחובר לאינטרנט, או בשירותי ענן עם הצפנה והזדהות חזקה - MFA).
עדכוני תוכנה ומערכת הפעלה - כל יצרנית תוכנה ומערכת הפעלה מפיצה מדי פעם עדכוני תוכנה ועדכוני אבטחה לתיקון כשלי מערכת או פרצות אבטחה שהתגלו. חשוב לבצע את עדכוני התוכנה מיד עם פרסומם. לרוב, הארגון מבצע עדכוני תוכנה וגיבויים בעמדות בארגון, אך לא תמיד זה מתאפשר במכשירים הניידים או הפרטיים שברשות העובדים. חשוב לוודא בארגון, כי אכן הוגדרו עדכונים אוטומטיים למערכות השונות.
התקנים חיצוניים - יש להימנע מחיבור התקנים חיצוניים ממקורות זרים ולהשתמש רק עם התקן קבוע פרטי, אשר אושר וסופק על ידי הארגון.
בדיונים רגישים, יש לוודא כי אין בחדר אמצעי מחשוב בעלי יכולת האזנה/הקלטה, טלפונים חכמים, שעון חכם, טלוויזיות, מצלמת מחשב ועוד.

הגנה על מכשירים בעת עבודה מחוץ למשרד

עובדים רבים משלבים עבודה מחוץ למשרד (יציאה לפגישות, אנשי שיווק ומכירות וכד'). מחשבים ניידים ומכשירים חכמים מאחסנים בתוכם מידע רב ומהווים "שער כניסה" פוטנציאלי עבור התוקפים השואפים לחדור לארגון. הגנה על אמצעים אלו ועל המידע המאוחסן בהם היא בעלת חשיבות גבוהה. רבים מהעובדים האלה נוהגים לעבוד מחוץ למשרד במקומות ציבוריים (בתי קפה, שדות תעופה, מלונות וכד'), ולכן חשוב להפגין ערנות רבה לסביבה שבה הם נמצאים. בעת עבודה במקום ציבורי יש להקפיד על הכללים האלה:

- לעולם אין להשאיר את המכשיר הארגוני או האישי ללא השגחה. די בהסרת המבט לרגע כדי שגורם עוין ינצל את ההזדמנות "להעלים" את המכשיר.
- חשוב לנעול את המכשיר באמצעות סיסמה חזקה, קוד, נעילת דפוס, אמצעי ביומטרי.
- חשוב להגדיר במכשיר נעילה אוטומטית לאחר אי-שימוש במשך זמן קצוב (רצוי לבחור כהגדרת מחדל את המינימום האפשרי).
- חשוב לבצע גיבויים לכל המכשירים ולמידע האגור בהם. כשעובדים מחוץ למשרד לא תמיד אפשר לבצע גיבויים, ולכן הכרחי לדרוש לבצע זאת. כך, במקרה של גניבה/פריצה/אבידה - ניתן יהיה לשחזר את המידע. חשוב להסביר, שניתן לבצע את הגיבוי להתקן חיצוני נייד או בענן.
- מומלץ להגדיר את תוכנת Find my phone, המאפשרת לאתר מכשיר שאבד/נגנב/נפרץ ואף לבצע מחיקת נתונים מרחוק.
- מודעות לסביבה - יש להסתיר את המסך מפני צפייה של זרים/עוברי אורח.
- יש להימנע ככל האפשר מלהתחבר ל-Wi-Fi מזדמן/ציבורי ולהעדיף להתחבר מרשת מאובטחת או מן המכשיר הנייד הפרטי (נקודת גישה אישית - Hot spot).
- בעת עבודה מחוץ למשרד או באזורים ציבוריים יש להימנע מעבודה על קבצים המכילים מידע חסוי/רגיש עסקי.
- יש להימנע מחיבור התקנים חיצוניים ממקורות זרים ולהשתמש רק עם התקן USB אישי. במידת הצורך, יש לבקש להעביר את הקבצים בדוא"ל.
- יש לוודא כי מותקנת במכשיר תוכנת אנטי וירוס (Anti-Virus) מעודכנת, אשר נועדה להגן על המחשב ועל המידע שנמצא בו. התוכנה מבצעת סריקה בניסיון לאתר וירוסים ואיומי מחשב שונים, תוך שהיא מונעת את חדירתם למכשיר.
- יש לוודא כי מותקנת במכשיר חומת אש מעודכנת, המשמשת כשער הגנה בין השרת לאינטרנט. חומת האש מאפשרת כניסה רק לגורמים שאושרו להיכנס

רבים מאתנו מורידים למכשירינו תוכנות ואפליקציות מהחנויות המורשות, בהן גם תוכנות אבטחה. חשוב להדגיש, כי גם תוכנות אלה הן לא תמיד ברמת אבטחה גבוהה, ולפני ההורדה למחשב חשוב לבחון את כמות ההורדות, את חוות דעת הגולשים וכד'.

ומונעת תקשורת לא רצויה או חדירה של גורמים מזיקים, כגון וירוסים, רוגלות, נוזקות וכד' אל המכשיר או למערכות הארגון.

בעת מסירת מכשיר של הארגון לעובד - חשוב לציין בפני העובד שעליו לנהוג משנה זהירות בשיתוף המכשיר המשמש לצורכי עבודה (מחשב/טלפון חכם) עם חבר או בן משפחה. מחקרים מראים, כי יותר מ-50% מהנתונים הרגישים ניתנים לגישה באמצעות הטלפון החכם או הטאבלט של העובד. בנוסף, התקנת אפליקציות היא קלה, וילדים לא חושבים פעמיים לפני הורדת יישום שנראה מושך.

המלצות הגנה על מכשירים פרטיים

לעתים אנו נאלצים להשתמש במכשירים הפרטיים שלנו לצורכי עבודה, למשל לצורך קריאת אי-מיילים ארגוניים או לביצוע שיחות והתכתבויות במדיות השונות. גם במקרים אלה אנו יכולים לשמש קורבן ליעד תקיפה - הן בהיבט האישי והן בהיבט הארגוני. להלן כמה טיפים, שיסייעו בהגנה על המכשירים הפרטיים ועל המידע האגור בהם:

- **נעילת המכשיר** באמצעות סיסמה/קוד/נעילת דפוס/אמצעי ביומטרי.
- הגדרת **אימות דו-שלבי** בכל אפליקציה או חשבון המאפשרים זאת.
- התקנת **עדכוני תוכנה למערכות ההפעלה של המכשירים -** מיד עם פרסומם.
- הגדרת **עדכוני תוכנה אוטומטיים** לכלל התוכנות/האפליקציות במכשירים.
- התקנת **תוכנת אנטי וירוס (Anti-Virus)**, אשר נועדה להגן על המחשב ועל המידע שנמצא בו. התוכנה תבצע סריקה עתית כדי לאתר וירוסים ואיומי מחשב שונים, תוך שהיא מונעת את חדירתם למכשיר.
- התקנת **חומת אש** מעודכנת, המשמשת כשער הגנה בין השרת לאינטרנט. חומת האש תאפשר כניסה רק לגורמים שאושרו להיכנס ומונעת תקשורת לא רצויה או חדירה של גורמים מזיקים, כגון וירוסים, רוגלות ונוזקות אל מכשיר.
- ביצוע **גיבויים** עתיים לכל המכשירים ולמידע האגור בהם. כך, במקרה של גניבה/פריצה/איבוד מכשיר - ניתן יהיה לשחזר את המידע. מומלץ לגבות בכמה מקומות, כגון התקן חיצוני ו/או בענן. בעת שמירה בהתקן חיצוני - יש לבצע את הגיבוי ולהבטיח ניתוק ההתקן מהמחשב ושמירתו במקום בטוח.
- הימנעות מהורדת אפליקציות ממקורות או מקישורים שאינם מוכרים, ולהורידן רק **מחנויות מורשות,** המספקות הגנה מסוימת מפני וירוסים (לדוגמה: App Store, Google Play, Microsoft Store). גם בחנויות מורשות חשוב להיות ערניים ולבדוק כי האפליקציות קיבלו משובים חיוביים וכי כמות ההורדות גבוהה.
- יש לבדוק מדי פעם בהגדרות המכשיר אילו הרשאות גישה אושרו בו לאפליקציות השונות (מיקום, מצלמה, מיקרופון וכד') ולהסיר **הרשאות מיותרות** שאינן רלוונטיות.
- **הימנעות מהורדה אוטומטית של קבצים** למכשיר (Autorun). ניתן להגדיר שהקבצים יורדו למכשיר רק לאחר לחיצה על הקובץ (למשל, באפליקציית WhatsApp, ניתן למנוע הורדת מדיה אוטומטית של קבצים, שמע, תמונות ווידיאו).

- **כיסוי עינית המצלמה** במכשיר כאשר לא נעשה בה שימוש. ניתן לעשות זאת באמצעות מדבקה ייעודית לכיסוי עינית המצלמה.
- בסיום השימוש במכשיר, חשוב לבצע **התנתקות מסודרת מכלל החשבונות**. הדבר נדרש בעיקר בעת מסירת המכשיר לתיקון במעבדה (חשוב לפנות לשירותי מעבדה מורשית).

שימוש במדיה נתיקה (USB)

אמצעי מדיה (מגנטית, נתיקה, אופטית, מכנית) משמשים לצורך הכנסה והוצאה של מידע מהארגון. אמצעי המדיה משמשים לאחסון וניוד מידע הן בתוך הארגון והן החוצה ממנו.
המחשב מאחסן בתוכו מידע רב ועלול לשמש כ"שער כניסה" פוטנציאלי של תוקף לתוך הארגון, ולכן יש להגן על מדיות נתיקות המכילות מידע רגיש.
תרחיש תקיפה שכיח מתרחש כאשר התוקף משאיר במקום גלוי DoK עם נושא מפתה כמו "משכורות"/"בונוסים"/"סודי ביותר", תוך הנחה שאחד העובדים יחבר אותו למחשב לשם איתור בעליו. לכן יש להימנע מלחבר התקנים חיצוניים ממקורות זרים או לא מוכרים, למשל התקני USB למיניהם, CD, Disk on Key, מטען או טלפון נייד וכד'. שימוש במדיה נתיקה תתאפשר רק:

- ❑ במקרה הצורך ובאישור הארגון
- ❑ ממדיה מהימנה וקבועה
- ❑ לאחר שעברה תהליך הלבנה[2]

חשוב להסביר, שטרם הכנסת קבצים ממקור כלשהו מחוץ לארגון לרשת הארגונית, יש לפנות לגורם אחראי בארגון, אשר יוכל לבדוק אותם ולאשרם. מומלץ לבקש מגורם חיצוני להעביר את הקבצים בדוא"ל על מנת שיעברו את הסינון הנדרש של הארגון.

[2] הלבנה - מערכת המבצעת תהליך של העברת קבצים מכל מקור מחוץ לארגון לתוך הרשת הארגונית. התהליך מאפשר ניטור ושליטה על החומר הנכנס לתוך הארגון באמצעות סוגים שונים של התקנים או תקשורות.

הגנה על הדואר האלקטרוני

הדוא"ל מהווה כלי עבודה משמעותי עבור כולנו ומשמש אמצעי תקשורת להעברת הודעות דרך רשת שרתים. מידע רב, בחלקו רגיש מאוד, נמצא בשרתי הדוא"ל - חלקו מצוי בתוך הארגון וחלקו בשירות חיצוני (למשל ענן). כדי להקטין את הסיכון לכך שגורם לא מורשה יוכל לקרוא התכתבויות ולפגוע במידע, חשוב להקפיד על הכללים האלה:

- חשוב להפריד חשבונות דואר אלקטרוני ולהגדיר דואר אלקטרוני אישי וארגוני.
- אין ללחוץ על הודעות או לפתוח צרופות חשודות, אשר הגיעו ממקור זר, או אפילו מוכר.
- אם התקבלה הודעה ממקור לא ידוע - אין למהר ללחוץ על קישורים או לפתוח צרופות. במקרים רבים תוקפים מתחזים לגורמים מוכרים, ולכן גם אם הדואר האלקטרוני התקבל ממקור מוכר, בדקו האם תוכנו רלוונטי טרם פתיחת קובץ או לחיצה על קישור. מומלץ לפנות ישירות לגורם לוודא שאכן הדוא"ל נשלח ממנו.
- לשמור על ערנות בהקשר להתחזויות ולמקור כתובת השולח - לעתים מגיע דוא"ל, אשר במקום כתובת מוכרת ותקינה כדוגמת: mydomain.co.il, הוא מגיע מכתובת שונה במקצת כדוגמת: mydomain.co או mydomain1.co.il, או paypa1.com במקום paypal.com
- יש לשים לב לבקשות בדוא"ל, המשדלות להעברת פרטים אישיים, תשלומים או העברת כספים ולוודא את אמינות בקשות התשלום בצורה ברורה מול הגורם המתאים. עדיף ליצור קשר עם הגורם השולח בערוץ תקשורת אחר (טלפון, SMS, WhatsApp, וכד') על מנת לוודא את אמינות הבקשה.

לדוגמה, "עוקץ מנהלים" - כאשר גורם עוין מתחזה למנהל בכיר בארגון ופונה באמצעות הדוא"ל למנהל אחד או לקבוצת מנהלים ומבקש לבצע העברה בנקאית.

- אין להעביר מידע ארגוני או רגיש לתיבת דואר אלקטרוני מחוץ לרשת הארגונית. במידת הצורך, יש להשתמש בפתרונות הצפנה לדואר אלקטרוני.
- אין להעביר/לשלוח שמות משתמש וסיסמאות בדואר אלקטרוני או בערוצים פומביים.
- בעת שליחת דואר אלקטרוני הכולל צרופה (Attachment), יש לוודא שהקובץ המצורף הוא אכן הקובץ שמיועד למשלוח.
- במשלוח דוא"ל לרשימת תפוצה נרחבת, חשוב לכתב את הנמענים בעותק נסתר BCC על מנת לא לחשוף את כלל כתובות הדוא"ל.

- בעת שימוש בסמארטפון הפרטי לקריאת מיילים ארגוניים, יש לוודא שהוגדרה סיסמת כניסה למכשיר. כמו כן, מומלץ להגדיר אימות דו-שלבי לצורך הפתיחה של תוכנת המיילים.
- במידה שעולה חשד לגבי קישור שהגיע, ניתן למקם עליו את סמן העכבר ולראות האם הוא אמין. ניתן גם להעתיק את הקישור ולהדביקו בשורת הכתובת בדפדפן שבמחשב - טרם לחיצה על Enter יש לבחון את הקישור לעומק ולבדוק האם יש סימנים מחשידים. אפשר להציג שוב את הדוגמה לדוא"ל חשוד בשקף 16.
- אם העובד כבר לחץ על הקישור או פתח את הצרופה - יש לוודא שההודעה לא נמחקה, על מנת שיהיה ניתן לתחקר אותה ולפנות מייד לאחראי המחשוב בארגון.

הכרחי להנחות את העובדים, שגם במצב שבו הם לחצו על הקישור או פתחו את הצרופה בתום לב - חשוב מאוד לא לחשוש לדווח. הסבירו, כי דיווח מידי של אירוע יכול למנוע נזקים חמורים עתידיים לארגון.

רבים מאיתנו מורידים למכשירינו תוכנות ואפליקציות מהחנויות המורשות, בהן גם תוכנות אבטחה. חשוב להדגיש, כי גם תוכנות אלה הן לא תמיד ברמת אבטחה גבוהה, ולפני ההורדה למחשב חשוב לבחון את כמות ההורדות, את חוות דעת הגולשים וכד'.

גלישה בטוחה באינטרנט

כולנו משלבים היום עבודה וחיים אישיים בגלישה ברחבי האינטרנט, הטומנת בחובה גם סכנות רבות. גורמים עוינים מחפשים דרכים להשיג נגישות למידע על משתמשים, ואחת הדרכים לכך היא יצירת אתרים מזויפים והפצת קישורים זדוניים ברשתות השונות, זאת במטרה להטעות את הגולשים להאמין שמדובר באתר רשמי. המטרה - לפתות אותם להזין פרטים אישיים, פרטי התחברות ואף פרטי כרטיס אשראי.

מובן שאין הכוונה להמליץ לא לגלוש ברשתות, אבל חשוב מאוד לבחון את כתובת האתר ולנסות לאתר סימנים מחשידים.

- אתר אינטרנט הוא אוסף של דפי אינטרנט מקושרים, שניתן לגשת אליהם דרך רשת האינטרנט על ידי הקלדת כתובת האתר בדפדפן. כתובת האתר (ה-URL) תהיה בדרך כלל שם המתחם (Domain Name) של החברה, השם הייחודי של האתר ברשת האינטרנט. לרוב, שם המתחם מזוהה עם שם של חברה/מוצר/מותג ידוע.
- יש לשים לב שהגלישה נעשית באתר מוצפן, שכתובתו מתחילה באותיות https (האות S מייצגת Secure - מאובטח), ולצד שמו מופיע סמליל של מנעול (מס' 2 באיור שלהלן). הדבר מציין, כי קיימת הצפנה של התעבורה בין דפדפן המשתמש לשרת המאחסן את האתר באמצעות תעודה דיגיטלית (SSL) מוכרת וכי מתבצע אימות, שהמידע נשלח בשלמותו ללא התערבות של גורם שלישי/עוין. חשוב להדגיש, כי אין זה מציין בהכרח שהאתר מאובטח, ויש לבדוק סימנים נוספים.
- ניתן להרחיב ולהסביר כיצד אפשר לבדוק תעודת SSL באתר (סמליל המנעול בדפדפן) ולבחון את הנתונים באמצעות לחיצה על המנעול ובדיקת הפרטים המופעים בחלון שנפתח: למי הונפקה התעודה, מי הגורם שסיפק אותה ומה תוקפה.
- חשוב לשים לב לעיצוב האתר - האם הוא מעוצב בצורה לא מקצועית, מופיעות בו שגיאות כתיב או ניסוח לשוני לקוי, מכיל קישורים רבים, או מרובה פרסומות.
- האם סיומת האתר מוזרה/חשודה? (מס' 4 באיור שלהלן).
- לפני שמקלידים פרטים אישיים באתרים השונים, יש לבדוק האם האתר מאפשר "יצירת קשר"/"פרטי התקשרות"/"Contact Us"/"מדיניות פרטיות"/"תקנון" (מס' 5 באיור שלהלן).
- בכל מקרה של חשש או חשד - יש להימנע מהזנה של פרטים אישיים או פרטי כרטיס אשראי באתר.


2
1
3
4
5
https://www.cyber.gov.il
gov.il
אתר השירותים והמידע הממשלתי
מערך הסייבר הלאומי
1. פרוטוקול – https\http
2. סמליל מנעול נעול/תעודת SSL
3. שם מתחם (דומיין) / שם האתר/URL
תואם לשם בלשונית הדפדפן
4. סיומת gov., .il, .org, .com.
5. מדיניות/אודות/פרטיות

רשתות חברתיות

הרשתות החברתיות השונות מסייעות לנו לעדכן מידע אישי, חברתי, משפחתי ומקצועי, לשתף תמונות, חוויות, חדשות ועוד. לצד היתרונות האלה טמונות גם סכנות רבות. הרשתות החברתיות מהוות כר פורה לאיסוף מידע מקדים, לריגול ולפיתוי. הפרטים והמידע שנחשפים ברשתות מלמדים את התוקף על דפוסי התנהגות, או על חולשות שבאמצעותן אפשר יהיה לתכנן ולבצע "הנדסה חברתית". באמצעות מודעות, ערנות והמלצות אלו ניתן למזער את הסכנות:

- יש לבחור סיסמה ארוכה ומורכבת ולבצע **אימות דו-שלבי** לכל חשבון המאפשר זאת.
- הגדרה בחשבון של קבלת התראות על התחברות לא מזוהה/מורשית.
- בהגדרות האבטחה אפשר להגדיר 3-5 אנשי קשר אמינים, שבאמצעותם יהיה אפשר לשחזר חשבון במקרה של חסימתו.
- יש לנקוט משנה זהירות בלחיצה על צרופות וקישורים, העלולים להכיל נוזקות או להוביל לאתרים מתחזים.
- בעת גלישה באינטרנט או ברשתות חברתיות עדיף להיות חשדנים - לא לשתף מידע אישי או מידע פנימי של הארגון בבלוגים, בטוקבקים, בפורומים או בכל ערוץ שיתוף אחר ברשת.
- רשימת עוקבים - יש לשים לב לפרטים שנחשפים בפני העוקבים ולהקפיד לצמצם את המידע שנחשף למינימום ההכרחי.
- ערנות וזהירות לגבי מפרופילים מתחזים/מזויפים - ייתכן שמדובר בדמות מתחזה או ברובוט. פרופילים אלו בדרך כלל כוללים מעט מאוד מידע, רשימת חברים מצומצמת, מעט תמונות או תמונות מקצועיות וברמה גבוהה מהרגיל, התבטאויות קיצוניות או דברי הסתה ועוד. מומלץ לא לאשר חברות אם אין חברים משותפים.

דיווח על אירוע חריג

חשוב להגדיר בארגון גורם אחראי, אשר ניתן לפנות אליו ולדווח לו בנושאים של אבטחת מידע.

יש להנחות את העובדים לפנות מיד לגורם האחראי בארגון במקרה של חשד או אי ודאות, במקרים האלה:

- **כאשר יש פגיעה ודאית או חשד לפגיעה באבטחת מידע.**
- **כאשר עולה חשד לתקלה תפעולית, אשר עלולה לגרום לפגיעה באבטחת המידע.**
- **כאשר יש חשד או זיהוי של פעילות חשודה של עמית או יריב.**
- **כאשר נגנב מחשב/ציוד קצה - שייך לארגון או מכשיר נייד אישי שבאמצעותו ניתן להיכנס למייל הארגוני.**
- **הימצאות של גורם חשוד או לא מורשה במתחם הארגון.**

במקרה של חשד לאירוע סייבר, ניתן לפנות 24/7 למרכז המבצעי לניהול אירועי סייבר במס' טלפון 119

נספח א' - ערכת המלצות התגוננות - להפצה בארגון

מערך הסייבר הלאומי כותב ומפרסם מסמכי הגנה ובקרה להתגוננות במרחב הסייבר. עמוד זה מפרט את הנושאים השונים שפורסמו עד ליום כתיבת מסמך זה. בנוסף, ניתן להירשם לקבלת עדכונים ברשתות החברתיות במטרה להתעדכן בפרסומים שונים לאזרח ולארגון.

ערכת המלצות להתגוננות	
שם המסמך	**קישור**
המלצות הגנה לצמצום סיכוני סייבר בתחנות קצה בארגון	https://www.gov.il/he/Departments/policies/endstation
התמודדות ארגונית במרחב הסייבר: האיום הפנימי	https://www.gov.il/he/Departments/General/coping_thret
עדכוני תוכנה	https://www.gov.il/he/departments/general/update_all_the_time
סיסמה חזקה	https://www.gov.il/he/departments/news/passwordrec
כיצד נזהה הודעות דיוג (Phishing)	https://www.gov.il/he/departments/general/fishingemails
התקפות דיוג (Phishing) - התחזות לספקיות שירות	https://www.gov.il/BlobFolder/reports/trip_fake/he/PHISHING-CERT-IL-W-966_1.pdf
לקראת רכישות ברשת	https://www.gov.il/he/departments/general/shopping_online
טיפים להגנה על הפרופיל האישי ברשתות חברתיות	https://www.gov.il/he/departments/news/safesocial
טיפים לקראת נסיעה לחו"ל	https://www.gov.il/he/departments/general/vacation_dont_forget
מדריך להגנה על תוכנות להעברת מסרים מידיים	https://www.gov.il/he/departments/guides/messaging

ניתן להתעדכן באתר מערך הסייבר הלאומי בהמלצות הגנת סייבר לאזרח והמלצות הגנה לארגון.