סייבר ישראל
מערך הסייבר הלאומי

כל מה שרציתם לדעת על מתקפות פישינג

המדריך המקיף של מערך הסייבר הלאומי

דצמבר 2021

מתקפות פישינג (דיוג) הן בין המתקפות הנפוצות והיעילות בשימוש תוקפים בעולם הסייבר ואף התעצמו מאז התפרצות הקורונה. פישינג עשוי להגיע כפנייה בדוא"ל, במסרון או בשיחת טלפון ולייצר לחץ למסירת פרטים תוך התחזות לגורם לגיטימי. בשנה האחרונה חלה עלייה בנסיונות ובמוקד 119 של מערך הסייבר הלאומי התקבלו כ-2,500 דיווחים בנושא, כאשר כל דיווח מעיד על עוד עשרות עד מאות אלפי הודעות דומות שנשלחו בישראל. שבוע הגנת הסייבר בישראל שמצויין בישראל, 12 עד 16 בדצמבר, נועד להעלות מודעות לנושא בקרב הציבור הרחב, לסייע לזהות את הסימנים המחשידים, להיזהר ולגלוש בטוח.

המתקפה עושה שימוש ברגשות אנושיים ושימוש בשיטות פסיכולוגיות שונות, מה שנקרא - הנדסה חברתית.

"הנדסה חברתית" היא ביצוע הונאה ומניפולציה באמצעות ניצול לרעה של מנגנוני ההתנהגות של האדם הממוצע. בדרך זו מנסים האקרים לשכנע לבצע פעולה העלולה לחשוף מידע רגיש או להריץ תוכנה זדונית במכשיר. כך למשל, הודעה על הצעת עבודה בלינקדאין מגורם מגייס של חברה מסוימת המכילה בקשה לביצוע פעולה כגון לחיצה והורדת קובץ או העברת פרטים אישיים ומידע רגיש אחר.

דיוג (פישינג- **Phishing**) היא אחת השיטות הנפוצות של הנדסה חברתית.
במתווה זה, לרוב, הפנייה נעשית לתפוצה רחבה של אנשים במסווה של גורם אמין (בדומה להטלת רשת של דייג) ובאמצעותה מנסים "לדוג ברשתו" מידע אישי או פיננסי. כאשר מקבל ההודעה מוסר שלא במודע את המידע או מבצע פעולה כגון לחיצה על לינק, פתיחת מסמך וכו', הוא נפל לפעולה זדונית ללא ידיעתו. פישינג יכול להתבצע באמצעות הדואר האלקטרוני, בשיחת טלפון, בשליחת מסרון ואף פנים אל פנים.

כדי להבטיח את הצלחת מתקפת הפישינג, מנסה האקר ליצור תחושות שונות בהן:

1. **הפחדה או דחיפות** - במטרה להוביל את המשתמש ללחוץ על קישור או קובץ במהירות וללא מחשבה מוקדמת. לדוגמה, שליחת הודעה ובה קריאה לעדכון פרטים אישיים בדחיפות פן ייחסם החשבון.
2. **ציפייה לקבלת פרס/הטבה** - הודעה כגון "100 הנרשמים הראשונים יזכו בסמארטפון מתנה" והפנייה להזנת פרטים אישיים.

3. **סקרנות** - שמטרתה לגרום למשתמש להוריד קובץ או ללחוץ על קישור מתוך סקרנות או גירוי. לדוגמה, הודעה על אישור רכישה שלא באמת בוצעה והזמנה ללחוץ על הקישור לצפייה בקבלה.
4. **אמפתיה** - שמטרתה להביא להזנת פרטים אישיים ופיננסיים. לדוגמה, יצירת תחושת הזדהות שתגרום לתרום כסף ע"י הזנת פרטי כרטיס אשראי או ביצוע העברה בנקאית.

דוגמה לעמוד דיוג:

קיבלתם הודעה משונה שפונה אליכם בשמכם, האם ייתכן שזה דיוג?

כן! זה נקרא **דיוג ממוקד (Spear Phishing)**. בסוג תקיפה זה מתבצעת פנייה מכוונת וממוקדת לאדם מסוים או לקבוצה ספציפית. התקיפה נעשית לאחר **איסוף מידע ורקע על אותם יעדים** הנוגע בעיקר לתפקידם בארגון ותחומי העניין שלהם כדי להפוך את הפניה אליהם למשכנעת במיוחד. למשל: הודעת דואר אלקטרוני מהמנהל המאשר לבצע עסקת תשלום לחברה שיש עימה קשר עסקי. ההודעה נראית אמינה ומרגישה לגיטימית, ומשכנעת לפעול לביצוע העברת התשלום - שהרי המנהל ביקש.

עצרו! היו חשדנים, בדקו את כתובת השולח, ודאו עם המנהל שאכן הוא זה ששלח את ההודעה בשיחת טלפון כדי לוודא שלא מדובר בדיוג ממוקד.

<u>מה הנזק שעלול להיגרם ממתקפות פישינג?</u>

- לחיצה על קישור בהודעה יכולה להוביל להורדת **תוכנה מזיקה למכשיר.**
- **העברת סכומי כסף** רבים במרמה.
- **השגת מידע** על הארגון או העובדים שיכול להוביל לתקיפות עתידיות.
- **חבלה** בעסקאות / בפעילות הארגון.

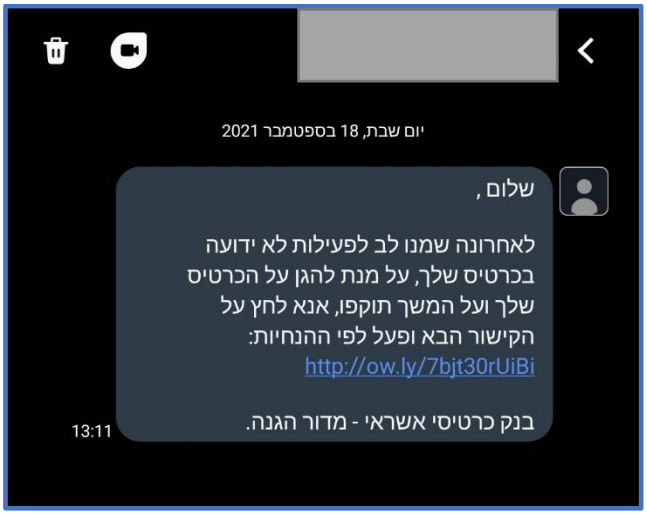
<u>מהם הסיכונים והסכנות?</u>

פישינג יכול להתבצע בצורות שונות:

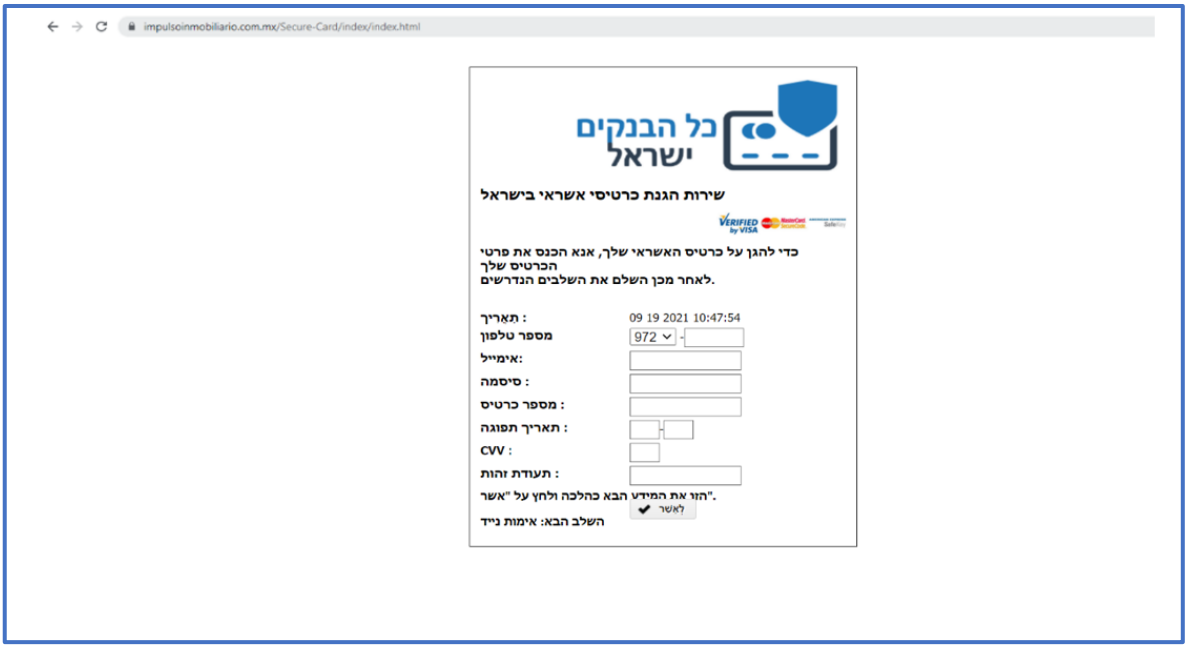
1. **הודעת טקסט ("סמישינג")**

ב-"סמישינג" התוקף שולח הודעה באמצעות SMS או כל אפליקציה אחרת להעברת מסרים ובה קישור עם קוד זדוני שלחיצה עליו תאפשר להאקר גישה לאותו המכשיר. אפשרות נוספת היא שהקישור יוביל לדף נחיתה בו דרישה להזין פרטים אישיים שיגיעו לידי ההאקר.

דוגמה לסמישינג:



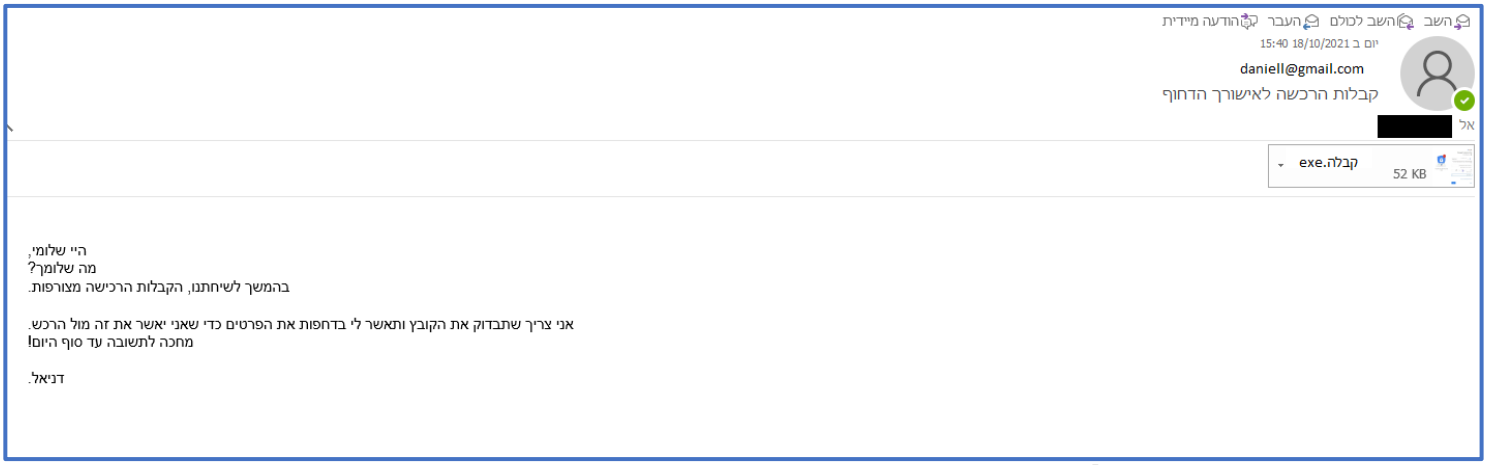
העמוד שייפתח לאחר הלחיצה על הקישור יכול להיראות כך:



2. **הודעות בדואר אלקטרוני**

בפישינג באמצעות הדואר האלקטרוני המטרה בדרך כלל להניע ללחוץ על קישור או הורדת קובץ. אם הקישור ו/או הקובץ זדוניים, לחיצה או הורדה של הקובץ מעניקה להאקר גישה אל אותו המכשיר או שהקישור יוביל אל דף נחיתה מתחזה, בו דרישה להזנת פרטים אישיים או פרטי הזדהות או התחברות.

דוגמה לפישינג בדואר האלקטרוני:



3. **תרמית הלוויתן- (whaling phishing)**

שיטה זו דומה לדיוג ממוקד, רק שכאן ההתחזות היא לגורם בכיר במטרה לגנוב כסף, מידע רגיש או לקבל גישה לרשת ולמערכות הארגון - כלומר מנסה לדוג דג גדול. זהו אלמנט מרכזי להפעלת לחץ על עובדים שעלולים לחשוש לסרב לבקשת מנהל או עובד בכיר.

לדוגמה: מנכ"לים בחברה שנמצא ממש על סף עסקת ענק עם חברה אחרת מקבל שיחת טלפון מהמנכ"ל של החברה השנייה או מגורם מוסמך מטעמה המאשר את העברת התשלום לשם השלמת העסקה. **עצרו**! מומלץ לוודא מי את זהות הגורם שמבקש או לנתק ולבצע אליו שיחה יזומה.
בפניות בדוא"ל, הניסוח לרוב יהיה בשפה העסקית כדי לא לעורר חשד.

4. **Business Email Compromise - BEC**

הונאות המבוצעות באמצעות דואר אלקטרוני במטרה להניע עובדים בארגון לבצע פעולות במרמה. הונאות אלה יכולות להישלח כהודעות דיוג בהן האקר מתחזה לספק, מגיש חשבונית לארגון ומנסה לגרום לעובד תחת לחץ זמן לבצע העברה בנקאית, לספק מידע או לאפשר גישה לרשת ארגונית.

5. **שיחות טלפון- וישינג/דיוג קולי (vishing/ voice phishing)**

בשיטה זו, ההאקר מתחזה באמצעות שיחת טלפון לגורם לגיטימי, מנסה לרכוש אמון ומבקש לבצע פעולות במסווה תמים כגון מסירת פרטים אישיים, פרטי התחברות או פרטים פיננסים. לדוגמה: טלפון מהבנק שמודיע על ביצוע עסקה חריגה בחשבון, ולשם ביטול העסקה אתם נדרשים לתת קוד אימות או את פרטי כרטיס האשראי שלכם.

עצרו! היו ערניים לבקשות חריגות בשיחות שלא יזמתם, כגון הצעות לרכישות טלפוניות.

6. **התחזות קולית בשיחת טלפון - Deepfake Voice Phishing**

התחזות במטרה להניע עובד לבצע פעולות כגון העברה כספית או לבצע פעילות זדונית ברשת הארגון. בשיטה זו, האקר אוסף מידע מקדים על הארגון הנתקף ואף משיג הקלטות קוליות של גורם בכיר בארגון במטרה להתחזות אליו. בהמשך, באמצעות שימוש בתוכנה ייעודית להתחזות קולית מתקשר ההאקר המתחזה אל עובד ומבקש ממנו לבצע פעולות כגון העברת כספים או פתיחת קובץ זדוני ברשת הארגונית.

7. **מודעות קופצות ופרסומות**
אם ברשת החברתית מופיעה מודעה - "לחצו על מנת להשתתף בהגרלה ואולי תוכלו לזכות בפרס". **עצרו**! לעתים לחיצה על מודעות קופצות ופרסומות באינטרנט יכולה להוביל להורדה של קובץ מזיק למכשיר. הורדת הקובץ מעניקה שליטה להאקר או מחדירה וירוס מזיק. לחיצה על המודעה גם עלולה להוביל לאתר מתחזה המבקש להזין פרטים אישיים.

8. **רשתות חברתיות**
בשיטה זו, האקרים מתחזים לדמויות שונות ברשתות החברתיות ובכך דולים מידע במרמה. מומלץ לגלות חשדנות להצעות חברות של פרופילים שאינכם מכירים, לבחון ולבדוק אם הם אמינים. בפרופילים מתחזים ו/או מזויפים תהיה בדרך כלל רשימת חברים מועטה, מעט תמונות, ציר הזמן יראה ריק וללא פעילות רבה.

9. **פנים אל פנים**
כל פעולה שבה אדם מבצע מניפולציה כדי להשיג פרטים שיוכלו לשמש אותו לתקיפת סייבר נקרא הונאת פישינג, זה עלול לקרות גם פנים אל פנים ולא רק במרחב הסייבר.

10. **הורדת אפליקציות**
בהורדת אפליקציות מהאינטרנט ולא דרך החנויות הרשמיות (App Store, Google Play) כגון אפליקציות חינמיות או קישור ישיר לאותו דף הורדות, קיים סיכון גדול. לעיתים, ההורדה מעניקה להאקר שלא במודע או בהסכמה גישה למכשיר שעלולה להזיק לו או לחשוף את הפרטים והמידע השמורים בו.

11. **מנועי חיפוש**
בשיטה זו, מעלים אתר אינטרנט ומאנדקסים אותו באופן לגיטימי במנועי החיפוש, במטרה להגדיל את רמת החשיפה שלו. אתרים אלה יכולים להיות אתרים מתחזים או אתרים עצמאיים. אתרים מתחזים מאופיינים בנראות אתר ודומיין דומים למקור. אתרים עצמאיים יציעו מוצרים ודילים במחיר משתלם במיוחד. כך, לא מתעורר חשד אצל הגולשים במנועי החיפוש.

לדוגמה: בעת כניסה לאתר, יתבקשו הרוכשים להשלים את העסקה באמצעות הוספת פרטי תשלום. פרטים אלה יועברו ישירות אל האקר שיצר את העמוד.

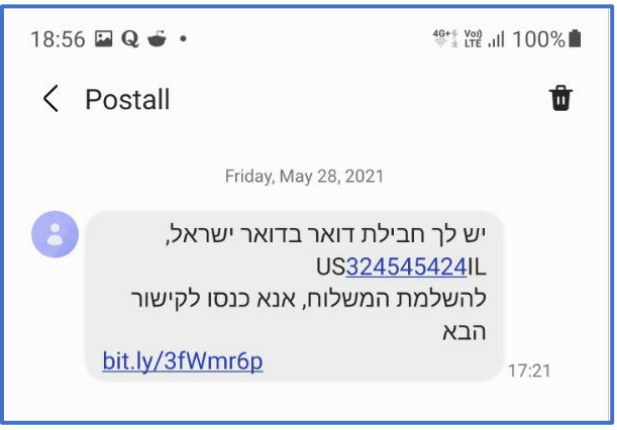
מהן הסיבות לביצוע מתקפות דיוג?

- **השגת מידע**- ניסיון להשיג מידע ישירות או לקבל גישה אל המידע ע"י שליחת קובץ או קישור זדוני.
- **השגת אפקט תודעתי או השפעה** - באמצעות הפצת מידע או מחיקתו (בעיקר באמצעות אתרים מזויפים ופרופילים מזויפים ברשתות החברתיות).
- **שיבוש, מניעה, מעקב או השבתה** - של מידע השמור על המכשיר.
- **רווח כספי**- התוקף ירצה להשיגפרטים פיננסים של הנתקף ובכך לקבל שליטה על חשבונו.
- **השתלטות על פרופיל ברשת חברתית** - במטרה לדרוש תשלום עבור שחרור הפרופיל או לחלופין על מנת להשתמש בפרופיל הקיים לצורך קידום אישי.
- **השבתת פעילות עסקית** - באמצעות נוזקה שתצפין את המידע, תמנע גישה אליו ותדרוש כסף תמורת שחרורו (כופרה).

כיצד לזהות מתקפות פישינג?

1. שימו לב **לכתובת השולח**, לרוב ארגון רשמי ישלח הודעה מכתובת לגיטימית של הארגון.
2. **תחושת דחיפות** - היו חשדנים כלפי דואר אלקטרוני הכולל קריאות לביצוע פעולות מידיות או ניסיונות ליצירת מצב של דחיפות. זו טכניקה נפוצה שנועדה לגרום לאנשים לפעול תחת לחץ ולגרום להם לטעות.
3. **"לקוח יקר"**- פנייה כללית שבה לא נעשה שימוש בשמו הפרטי של הלקוח, צריכה להדליק נורה אדומה.
4. כתובת מתחזה - מיקום או ריחוף העכבר מעל הקישור יציג לנו את הכתובת האמיתית של הקישור. בעת קבלת קישור המציע לבצע פעולה כלשהי באתר, גם אם הוא נראה מוכר, כדאי לגשת אליו באופן יזום דרך הדפדפן ולא דרך הקישור שנשלח בהודעה.
5. **שגיאות כתיב** - בחנו היטב את ההודעה ושימו לב לשגיאות כתיב/ניסוח לקוי.

6. **הצעות מפתות** - הודעות המכילות הבטחות או הצהרות בלתי סבירות הן בדרך כלל כאלו - לא סבירות ומזויפות. כך למשל הבטחה לזכייה במוצר נחשק, הגרלה או הטבה משמעותית.
7. **הודעה שלא ציפיתם לקבל -** האם שם השולח מוכר לכם? האם שוחחתם על כך? שימו לב כי כתובת השולח ושם השולח תואמים.
8. קובץ הרצה - היו חשדנים כלפי צרופות (קבצים למיניהם). פתחו רק צרופות המגיעות ממקור או מכתובת דואר אלקטרוני של שולח שציפיתם לו. אם אינכם בטוחים תוכלו לסרוק את הקובץ בתוכנות ושירותים ייעודיים לבדיקת קבצים או לחלופין צרו קשר עם השולח באמצעי תקשורת אחר (בדיקה באתר, פנייה טלפונית וכו').
9. **אל תספקו מידע**- שימו לב כי חברות לא יבקשו מכם פרטים אישיים כמו סיסמה או פרטי כרטיס אשראי (אלא אם כן אתם רוכשים באינטרנט או נרשמים לשירות מיוזמתכם האישית). לכן, אל תמהרו לספק פרטים אלו - היו חשדנים!
10. **שימוש בקישור מקוצר**- תוקפים רבים משתמשים בקישורים מקוצרים בכדי להסתיר את הכתובת האמיתית אליה הם מפנים. כדי להיות בטוחים תוכלו לבדוק את הקישור המקורי באתרים המאפשרים זאת, או באמצעות הדרכים שהוזכרו לעיל. אין ללחוץ על קישורים חשודים, הם יכולים להכיל קובץ זדוני או להפנות לעמודי דיוג.



***זכרו**! קישור מקוצר אינו בהכרח זדוני ומשמש שירותים וחברות לגיטימיים במקרים רבים.

<u>מה עושים במידה ונפלתם ברשת?</u>

- **תוכנות הגנה ייעודיות** - אם פתחתם קישור שנראה לכם חשוד, השתמשו בתוכנות ושירותי הגנה ייעודיים כדוגמת אנטי וירוס, חומת אש, מערכות לגילוי/מניעת חדירות ועוד.
- **החלפת סיסמה** - במקרה ומסרתם את הסיסמה שלכם, מומלץ לשנותה בכל החשבונות לסיסמה ארוכה ומורכבת - אורך של 10 תווים ומעלה עם שילוב של מספרים, אותיות גדולות, קטנות ותווים מיוחדים. כמו כן, תוכלו להשתמש בתוכנות ייעודיות ליצירת סיסמאות מורכבות.

- **אימות דו- שלבי** - מומלץ להגדיר אימות דו שלבי/רב גורמי בכל חשבון שמאפשר זאת.
- **עדכון הבנק וחסימת הכרטיס** - במידה ומסרתם את פרטי חשבון הבנק או כרטיס האשראי שלכם כדאי להיות בקשר עם הבנק ולעדכן אותו לגבי המקרה וכן לחסום או להשהות את הכרטיס.

באילו כלי תקיפה התוקפים משתמשים?

- **נוזקה (Malware)-** נוזקה היא שם כולל לתוכנות המזיקות למחשב ומשמשות למימוש תקיפת סייבר. קיימות מגוון סוגי נוזקות דוגמת- וירוס, תולעת מחשב, כופרה, KEYLOGGER ועוד.
- **רוגלה (Spyware)-** נוזקה המשמשת לגניבת מידע.
- **וירוס (Virus)-** נוזקה החודרת למחשב באופן סמוי, משתמשת במשאבי המחשב להעתיק ולהפיץ את עצמה, ולרוב פוגעת בפעולה התקינה של המחשב הנגוע.
- **סוס טרויאני (Trojan Horse)-** כינו לנוזקה שמטרתה לחדור למחשב תוך התחזות לתוכנה תמימה.
- **כופרה- (RansomWare)-** נוזקה המונעת את היכולת להשתמש במשאבי מחשוב באמצעות הצפנת המידע האגור במחשב ומשמשת לצרכי סחיטה.
- **תולעת מחשב** (Worm)- היא נוזקה המשכפלת את עצמה דרך הרשת, ומדביקה מחשבים אחרים.

אילו פעולות ניתן לעשות כדי להיות בטוחים יותר?

- **היו קנאים לפרטיותכם** - לגורמים עוינים, כמו לכולם, יש גישה למידע פומבי ברשתות החברתיות שעשוי להיות מנוצל כדי להפוך את ההונאה למתוחכמת ומשכנעת יותר. לכן נסו לשמור כמה שיותר על פרטיותכם. היו ערניים למה שאתם מפרסמים ברשת, מומלץ גם לשמור על החשבונות שלכם ברשתות החברתיות נעולים, להגדיר הגדרות פרטיות ולאשר רק אנשים שאתם מעוניינים שיראו את התוכן שאתם מעלים.
- **סיסמאות מגוונות** - הגדירו סיסמאות שונות ומגוונות לכל אחד מהחשבונות שלכם, כך במקרה שהצליחו "לדוג" סיסמה לחשבון אחד, לא יהיה ניתן לפרוץ לחשבונות האחרים.
- **הפעילו אימות דו שלבי/רב גורמי** - על כל חשבון שמאפשר זאת, כך שגם אם מסרתם אימות מזהה אחד, התוקף יצטרך אמצעי זיהוי נוסף כדי להיכנס לחשבון שלכם.

- **התקינו מוצרי אבטחה טובים ואיכותיים במחשב ובטלפון -** שימוש במוצרים אלה מועיל מאוד בהגנה על המכשירים במקרה של תקיפות פישינג.
- **הורדת אפליקציות מחנויות רשמיות** - מומלץ להוריד אפליקציות רק דרך החנויות המוכרות (Google Play, Appstore).
- **סינון ספאם** - פלטפורמות מסוימות של דואר אלקטרוני, ינווטו אוטומטית הודעות שנראות להן בעלות כוונת זדון לתיבת דואר ספאם. בנוסף, קיימת האפשרות לדווח על הודעות שאבחנתם כחשודות כהודעות ספאם.
- **כתובת אתר מאובטחת** - שימו לב שכתובת האתר מתחילה בhttps (ה-s מכוון ל-Secure, מאובטח) ולצדה יוצג סמליל של מנעול סגור, המסמל שמדובר באתר מאובטח. ואולם, יש מתקפות פישינג המשתמשות גם בכתובת מאובטחת.
- **כתובת משובשת** - במידה וקיבלתם הודעה מפתה או מוזרה המכילה קישור בדקו: האם הכתובת מדוייקת, האם יש הטעייה, שיבוש מילה או מיקום האותיות השתנה וזה בעצם רק דומה לאתר המקורי.
- **להתקשר ישירות לפונה** - אם אתם חושדים כי מנסים להוליך אתכם שולל דרך שיחה טלפונית- נתקו את השיחה והתקשרו ישירות לגורם הפונה, על ידי חיפוש פרטיו באתר רשמי.

המלצות הגנה לארגונים

העלאת המודעות בקרב עובדי הארגון

- **תרגילי דיוג-** אחת לחודש או תקופה, יישלח מייל לעובדי הארגון אשר ידמה מתקפת דיוג. באמצעות מייל זה ניתן לבחון כמה עובדים נפלו ברשת ועד כמה גבוהה מודעות העובדים למתקפות דיוג. השאיפה היא כי כמות הלחיצות של העובדים תפחת עם הזמן (מתרגיל לתרגיל) .
- **קיום תרגילים תקופתיים-** לעובדים ממגוון תפקידים לצורך ריענון הנהלים.
- **הדרכה ממוקדת-** אחת לרבעון תוצג מצגת מטעם מחלקת אבטחת מידע לאוכלוסיות שונות /מחלקות שונות על מנת לרענן את ההנחיות ולהציג פילוח סטטיסטיקות ומקרים אמיתיים שקרו בארגון. מומלץ גם לבצע הדרכת עובדים חדשים עם כניסתם לארגון.

ערכת הדרכה בנושא איומי סייבר ואבטחת מידע :

https://www.gov.il/he/Departments/General/instructiontools

- **<u>שבוע הגנת סייבר</u>** - ניתן להפיק שבוע הגנת סייבר פנים ארגוני או לחלופין לשתף פעולה עם שבוע הגנת הסייבר שמקיים מערך הסייבר הלאומי.
- **<u>לומדה</u>** - מומלץ כי כל עובד ישתלם באמצעות לומדה בנושא פישינג באופן תקופתי או עם כניסתו לארגון.

כניסה ללומדת התנהלות בטוחה במרחב הסייבר עבור עובדים בארגונים:

https://www.gov.il/files/cyber/Workers-WEB/story_html5.html

כניסה לקורס מקדם הגנה בסייבר:

https://campus.gov.il/course/course-v1-cs-csdefence001/

- **<u>שומרי מסך</u>** - יצירת שומרי מסך ייעודיים לנושא אשר ישתנו אחת לחודשיים.

במידה וקיבלתם הודעת פישינג בחשבון הדואר האלקטרוני של העבודה כדאי לבצע בנוסף את הפעולות הבאות:

- אם המייל התקבל על מכשיר או לחשבון של הארגון, כדאי לפנות לאחראי המחשוב בארגון וליידע אותם אודות המקרה.
- חשוב להנחות את העובדים להפריד בין תיבת הדואר האלקטרוני המשמשת לפעילות עסקית לבין זו המשמשת לפעילות הפרטית, כך שבמקרה של פגיעה בחשבון הפרטי לא תהיה השפעה על החשבון הארגוני / עסקי.

<u>מערכות ויכולות ההגנה ייעודיות</u>

- **מערכת לסינון דוא"ל** (ESG - Email Security Gateway) - מערכת טכנולוגית אשר מטרתה לאתר ולהסיר מהודעות דוא"ל נוזקות וקישורים זדוניים. כמו כן, המערכת מסוגלת לצמצם את כמות "דואר הזבל" (Spam) אשר הארגון מקבל מהאינטרנט.
- מומלץ להוסיף **כיתוב בולט** לכל הודעת דוא"ל אשר מתקבלת ממקור חיצוני המבהירה למשתמש כי אין מדובר בהודעה אשר נשלחה מגורם פנים ארגוני. ככל שהכיתוב יהיה בולט וצבעוני יותר, סביר להניח כי הדבר יעלה את מודעות המשתמש ויצמצם את הסתמכותו על תוכן הדוא"ל.
- **מערכת לתרגול ומודעות משתמשים** (Security Awareness and Training) - מערכת טכנולוגית אשר מטרתה לתרגל ולקדם מודעות משתמשים לאיומי סייבר שונים דוגמת פישינג.
- **מנגנון האבטחה לאימות זהות השולח** (DMARC) אשר יצמצם משמעותית את הסיכונים לפתיחת דוא"ל מתחזה ויאפשר לקבל הודעות דואר אלקטרוני בבטחה. DMARC מבטיח כי הודעות דואר אלקטרוני שמתקבלת משולח שזהותו אינה מאומתת, יחסמו ולא יגיעו אל יעדם ומטרתו היא מניעת גניבת פרטי הזדהות, פרטי כרטיסי אשראי, הפצת תוכנות נוזקה, קבלת גישה

לחשבונות משתמשים בעסק - פעולות שעלולות להוביל לנזק משמעותי לעסק ולעובדים.

לפרטים נוספים אודות ה- DMARC:

https://www.gov.il/he/departments/news/dmarc_pmi

==========

ולסיום, מומלץ להיעזר בטיפים ובדרכי הזיהוי שמובאים במדריך ולשמור על ערנות כדי להיות מוגנים כמה שיותר. ואם בכל זאת נתקלתם במשהו חשוד ואינכם בטוחים, תוכלו להסתייע ולדווח למרכז הארצי לניהול אירועי סייבר של מערך הסייבר הלאומי בחיוג ישיר 119, ובכך אף תוכלו לסייע במניעת הפצה רחבה של מתווה זדוני או תקיפה.