סייבר ישראל
מערך הסייבר הלאומי

איומי סייבר ואבטחת מידע
הדרכה לעובדים

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 העמידות בסייבר במשק ובלבד שישמר הייחוס למערך הסייבר הלאומי כפי שמופיע בערכת ההדרכה. כל הזכויות שמורות למערך הסייבר הלאומי. המלצות ההגנה יתעדכנו מעת לעת ובאחריות המשתמשים בערכת ההדרכה לעקוב אחר העדכונים.
אין להוסיף סמלילים לצד הסמליל של מערך הסייבר הלאומי. כל שינוי אחר שיתבצע במצגת הוא באחריות הארגון בלבד ואין ליחסו למערך הסייבר הלאומי.
מומלץ שגורם מקצועי בארגון (מנהלי אבטחת המידע/ CISO, מנמ"רים, 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: Awaerness@cyber.gov.il.

מטרת ההדרכה

- הכרה והבנה של איומים וסכנות הטמונים בפעילות במרחב הסייבר.
- הכרת כלים והמלצות בסיסיות שיסייעו לצמצם פגיעה עקב פעילות במרחב הסייבר האישי והארגוני.
- הכרת הגורם המקצועי שניתן לפנות אליו ו/או לדווח לו במצב חירום.

תוכן

אחריות העובד/ת בארגון

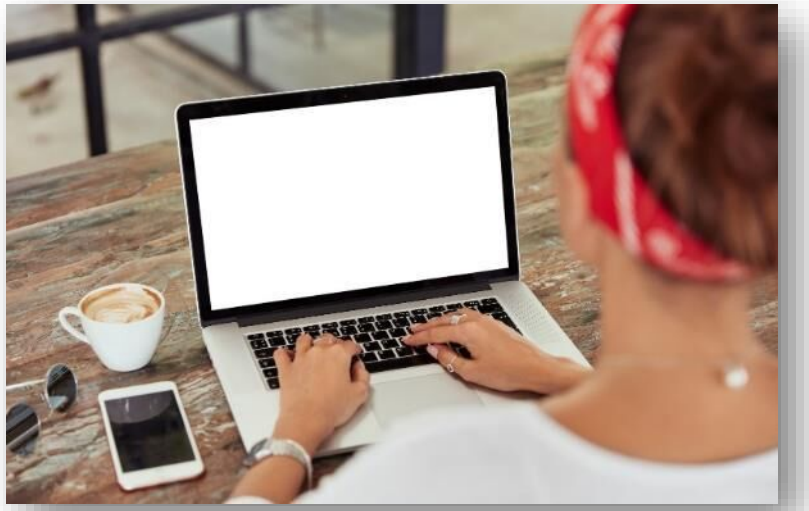
מהי תקיפת סייבר?

השגת שליטה ללא רשות במערכת מידע

גורמי איום ובעלי עניין במרחב הסייבר

»»» כיצד מתרחשת חדירה לארגון

תחנת הקצה



הגורם האנושי

לרוב, התקיפה תתבצע על תחנת קצה ברשת באמצעות התנהלות אישית לקויה
(פתיחת קישור, הורדת קובץ, הכנסת DOK וכד')

שלבי מתקפת סייבר

- איסוף מידע
- חדירה ראשונית
- התבססות
- התפשטות
- פגיעה

לא כל מתקפת סייבר פועלת עפ"י שלבים אלו. התוקף יבחר שלבים בהתאם למטרת התקיפה, הזמן והמשאבים העומדים לרשותו.

סוגי נוזקות נפוצות

תולעת

וירוס

סוס טרויאני

רוגלה

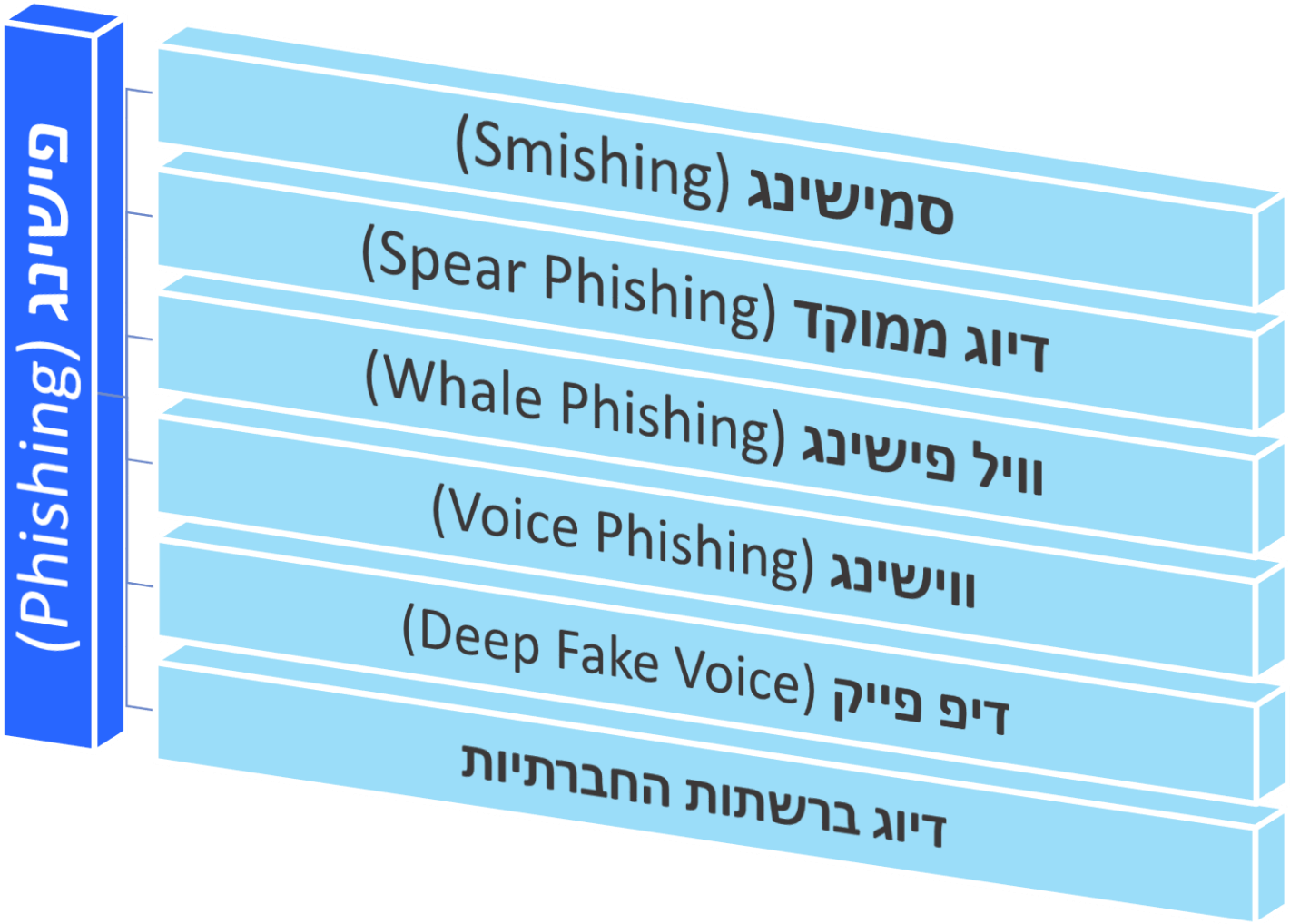
סייבר ישראל
מערך הסייבר הלאומי

שיטות תקיפה

הנדסה חברתית

Social Engineering

דיוג (פישינג)



כל אחד עלול בקלות ליפול קורבן!

חשוב מאוד! אם לחצתם על קישור

ו/או מסרתם פרטים - דווחו מיד לגורם

האחראי בארגון

חשוד או לא?

נשלח מ: DHL Deliveery <DHL-Deliveery@gmail.com>

כותרת: חבילה שמספרה N39371848IL ממתינה לאיסוף

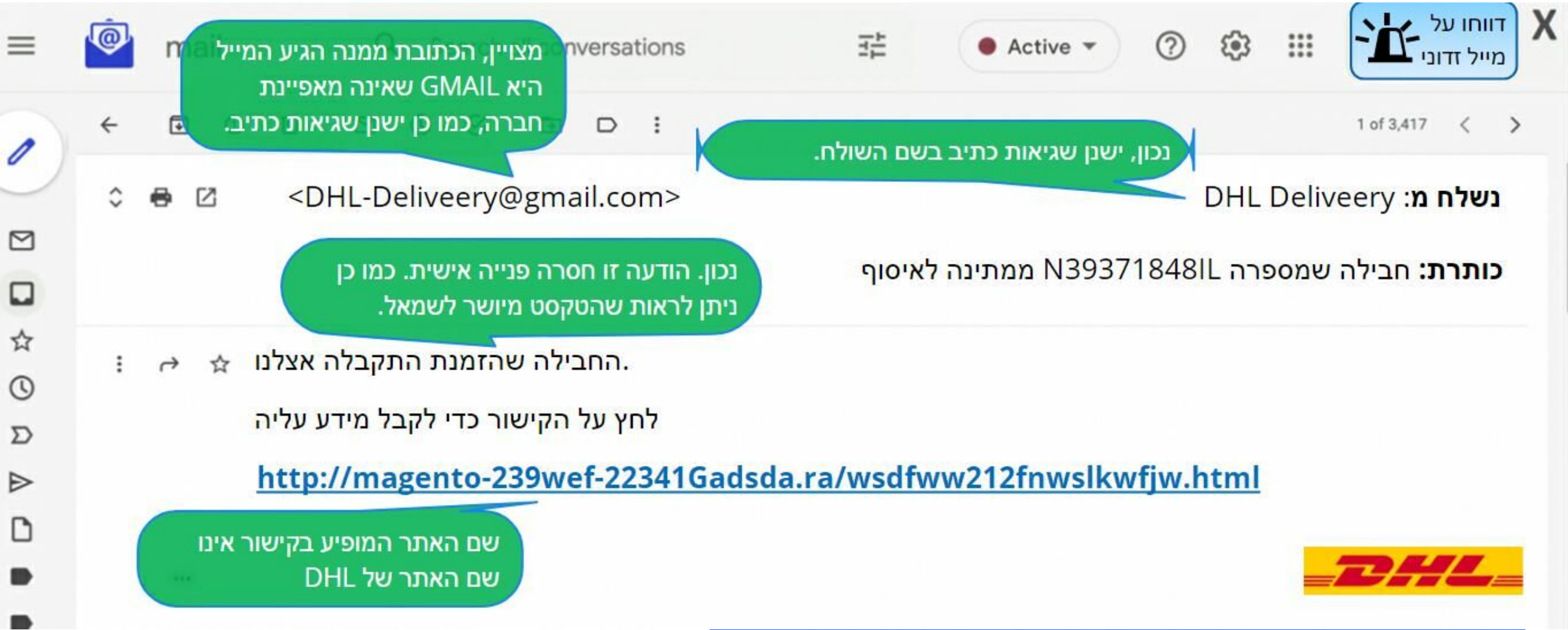
החבילה שהזמנת התקבלה אצלנו.

לחץ על הקישור כדי לקבל מידע עליה

http://magento-239wef-22341Gadsda.ra/wsdfww212fnwslkwfjw.html

Reply Forward

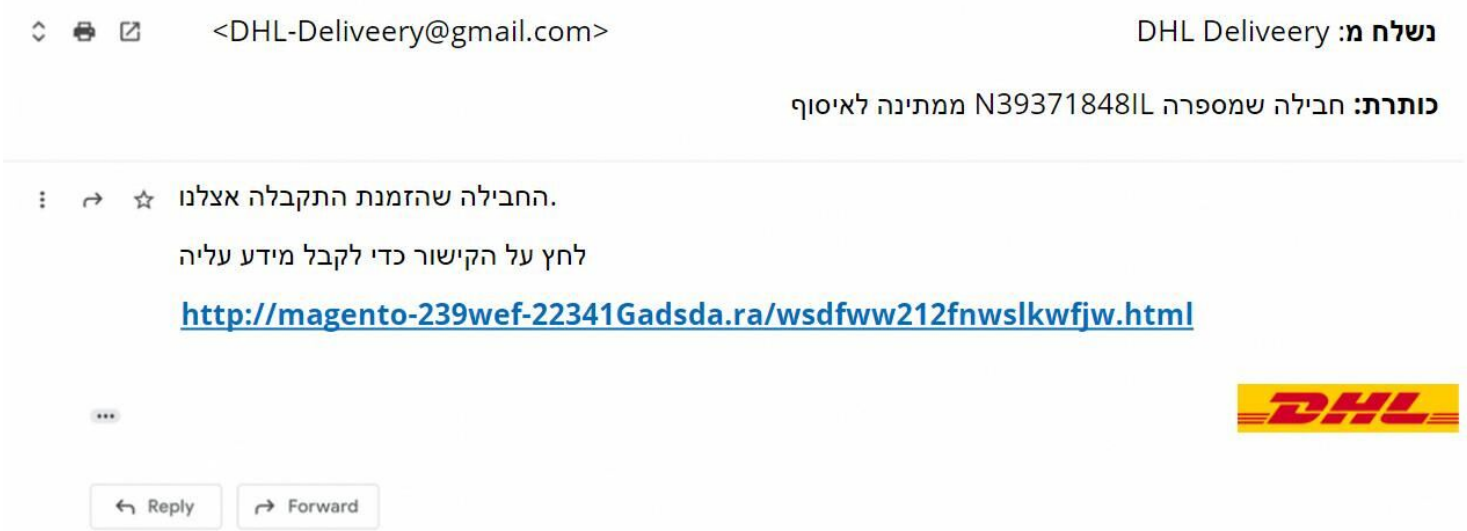
חשוד או לא?


דווחו על מייל זדוני
Active
1 of 3,417
מצויין, הכתובת ממנה הגיע המייל היא GMAIL שאינה מאפיינת חברה, כמו כן ישנן שגיאות כתיב.
נכון, ישנן שגיאות כתיב בשם השולח.
נשלח מ: DHL Deliveery <DHL-Deliveery@gmail.com>
כותרת: חבילה שמספרה N39371848IL ממתינה לאיסוף
נכון. הודעה זו חסרה פנייה אישית. כמו כן ניתן לראות שהטקסט מיושר לשמאל.
החבילה שהזמנת התקבלה אצלנו.
לחץ על הקישור כדי לקבל מידע עליה
http://magento-239wef-22341Gadsda.ra/wsdfww212fnwslkwfjw.html
שם האתר המופיע בקישור אינו שם האתר של DHL

אז איך מתגוננים מפני פישינג?

אז איך מתגוננים מפני פישינג?

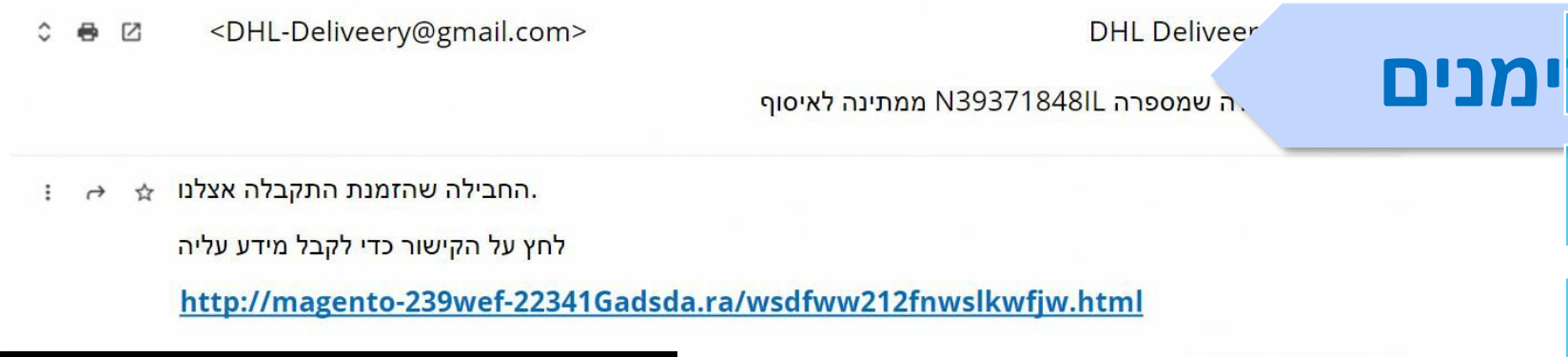
מחפשים את הסימנים

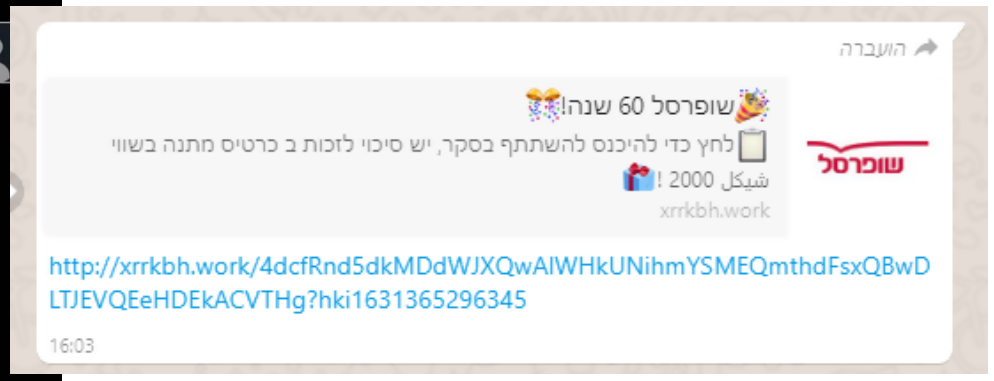


אז איך מתגוננים מפני פישינג?

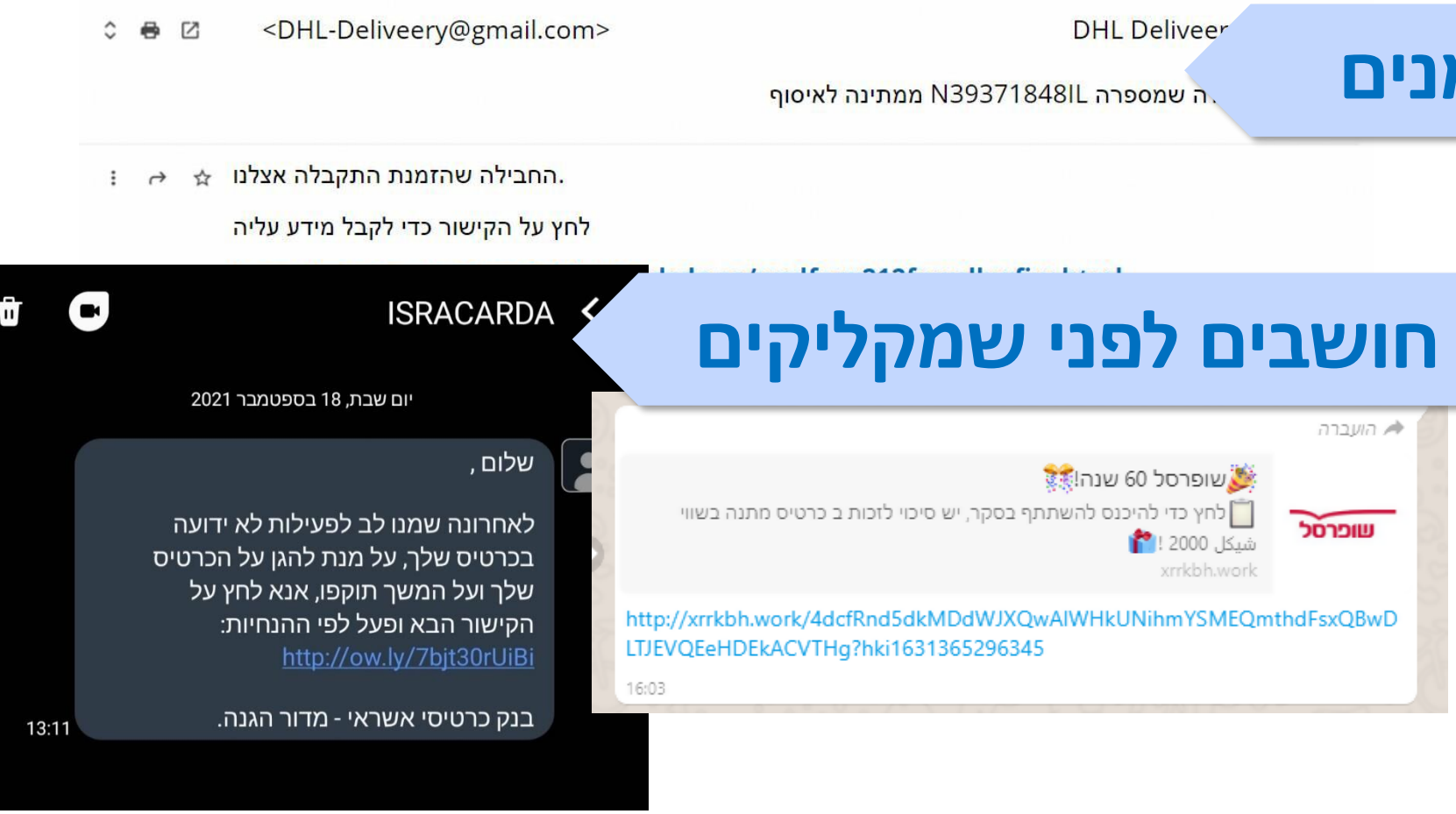
מחפשים את הסימנים

- כתובת השולח
- יצירת תחושת לחץ/דחיפות
- היעדר פנייה אישית
- נוסח חובבני, שגיאות כתיב, שילוב שפות, יישור טקסט לשמאל
- "מתנות חינם"
- כתובת הקישור אליו מפנים
- בקשה להזנת פרטים או הורדת קובץ





אז איך מתגוננים מפני פישינג?

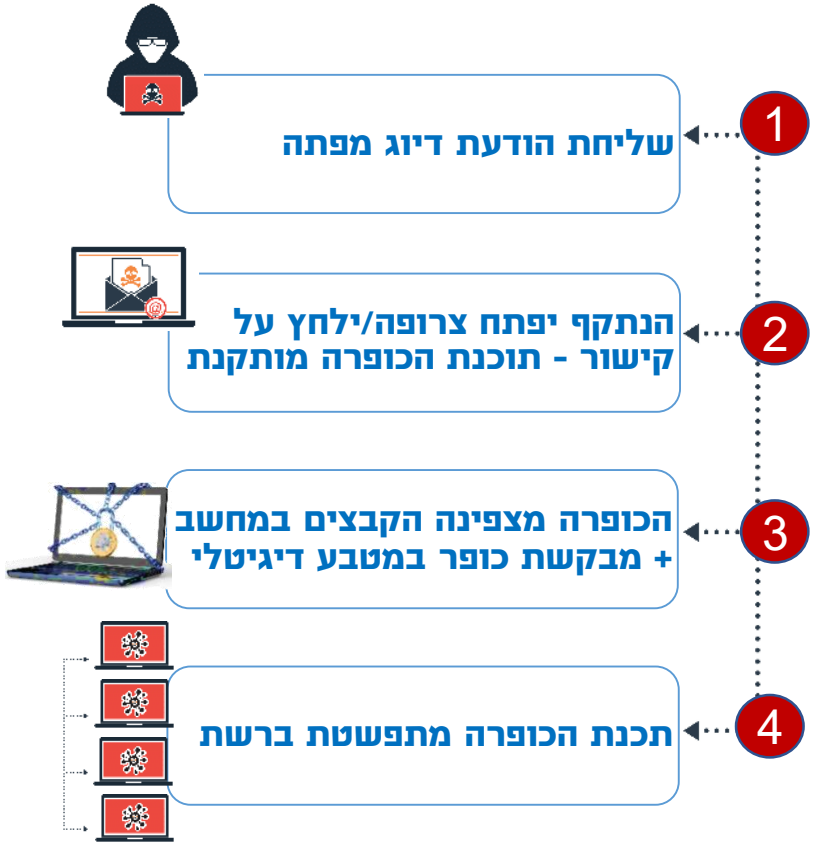


מתפשים את הסימנים

חושבים לפני שמקליקים

- כתובת השולח
- יצירת תחושת לחץ/דחיפות
- היעדר פנייה אישית
- נוסח חובבני, שגיאות כתיב, שילוב שפות, יישור טקסט לשמאל
- "מתנות חינם"
- כתובת הקישור אליו מפנים
- בקשה להזנת פרטים או הורדת קובץ

מתקפת כופרה (Ransomware)



No More Ransom

הידעתם? תשלום הכופר לא בהכרח יוביל את התוקף לשחרר את ההצפנה.

סייבר ישראל
מערך הסייבר הלאומי

המלצות בסיסיות להתגוננות

המלצות הגנה

הנדסה חברתית -דיוג

סיסמאות
ואימות דו שלבי

הגנה על מכשירים

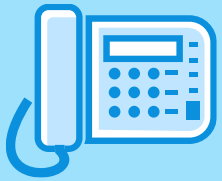
הגנה על מכשירים
אישיים

מדיה נתיקה

דואר אלקטרוני

גלישה באינטרנט

רשתות חברתיות



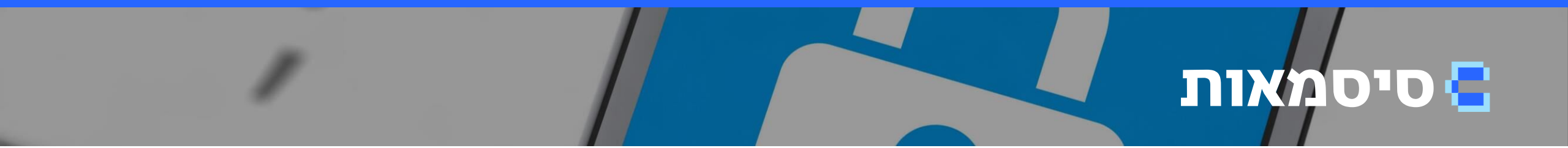
דיווח אירוע

סייבר ישראל
מערך הסייבר הלאומי

מהי סיסמה חזקה?

QWERTY123

סיסמאות



- בחרו בסיסמה ארוכה המורכבת מביטוי/משפט, שלבו בה אותיות גדולות וקטנות, ספרות וסימנים מיוחדים, כמו !#$@.
- הימנעו מבחירה ב**סיסמה נפוצה**, או כזו המבוססת על מידע גלוי שלכם (תאריך לידה, שם ילד/חיית מחמד וכד').
- בחרו ב**סיסמאות שונות** לכל חשבון שברשותכם.
- שמרו את הסיסמאות ב**מקום בטוח** ולא בקרבת המכשיר. מומלץ לשנן או להצפין את הסיסמה.
- לעולם **אין לחשוף סיסמה לאף אחד**! גם לא לספק או גורם המזדהה עם הארגון.
- הגדירו **אימות דו שלבי/רב גורמי** בכל חשבון המאפשר זאת.
- אם עלה חשד שסיסמתכם נחשפה, יש לשנות אותה מיד בחשבונות השונים.
- ניתן להשתמש ב**מנהל סיסמאות**, המאפשר שמירת כל הסיסמאות ב"כספת", כאשר עליכם לזכור רק סיסמה אחת.

סייבר ישראל
מערך הסייבר הלאומי

אימות דו שלבי

מצמצם משמעותית את הסיכוי
לפריצה לחשבון

אימות דו שלבי (2FA)

תהליך ההזדהות מורכב משני שלבים:

1. **זיהוי**
2. **אימות** - באמצעות:

- **מידע שהמשתמש יודע** (Something you know)
- **מידע על המשתמש עצמו** (Something you are)
- **שימוש במכשיר הספציפי הנמצא ברשותו של המשתמש** (Something you have)

אימות רב-גורמי (MFA) - שימוש בשני גורמים או יותר

טיפים להגנה על מכשירים במשרד ומחוצה לו

הגנה על מכשירים במשרד

בכל יציאה שלכם מהמשרד או בסיום יום העבודה, התנתקו מהחשבונות הדיגיטליים ונעלו את המחשב (Ctrl+Alt+Delete - נעל).

יש לנעול את המחשב הנייח או הנייד באמצעות סיסמה, קוד, נעילת דפוס*, אמצעי ביומטרי.

* דוגמה לנעילת דפוס

ודאו בארגון כי אכן מתבצעים גיבויים עיתיים במחשב ובמכשירים הניידים שברשותכם. ודאו תקינות הגיבויים וכן שמירה עיתית לא מקוונת של גיבויים.

מומלץ לוודא כי במחשב הוגדר עדכון אוטומטי למערכת הפעלה, לתוכנות ולדפדפן.

הימנעו מלחבר התקנים חיצוניים ממקורות זרים. השתמשו רק בהתקן קבוע משלכם, אשר אושר וסופק ע"י הארגון.

לרוב, הארגון מבצע עדכוני תוכנה וגיבויים בעמדות קצה בארגון, אך לא תמיד זה מתאפשר במכשירים הפרטיים שברשותכם. לכן, מומלץ לבצע עדכונים וגיבויים לכל המכשירים שברשותכם.

הגנה על מכשירים בעת עבודה מחוץ למשרד

- לעולם אין להשאיר את מכשירכם ללא השגחה!
- יש לנעול את המכשיר באמצעות סיסמה, קוד, נעילת דפוס, אמצעי ביומטרי. הגדירו נעילה של המכשיר לאחר חוסר שימוש של x דקות.
- חשוב לבצע גיבוי לכל המכשירים שברשותכם ולמידע האגור בהם. כך, במקרה של גניבה/פריצה/אבדה - ניתן יהיה לשחזר את המידע. ניתן לגבות בהתקן חיצוני או בענן (ודאו שספק הענן מצפין את המידע ומספק FA2).
- מומלץ לעדכן את יישום Find my phone המאפשר לאתר מכשיר שאבד/נגנב/נפרץ ואף לבצע מחיקת נתונים מרחוק.

- בעת עבודה במקום ציבורי, דאגו להסתיר את המסך מפני צפייה של זרים / עוברי אורח.
- הימנעו מלהתחבר לרשת Wi-Fi ציבורית/חינמית. העדיפו להתחבר מרשת מאובטחת או ממכשיר הנייד (נקודת גישה אישית/Hotspot).
- מחוץ למשרד, הימנעו מלעבוד על קבצים המכילים מידע חסוי/רגיש עסקי.
- הימנעו מלחבר התקנים חיצוניים ממקורות זרים. השתמשו רק עם התקן קבוע משלכם. במידת הצורך, בקשו להעביר אליכם קבצים בדוא"ל (רוב ספקי הדוא"ל מבצעים סינון מסוים).

סייבר ישראל
מערך הסייבר הלאומי

על המכשיר האישי שלך כבר הגנת?

חברו הטוב של האדם

הגנה על מכשירים פרטיים

לעתים אנו נאלצים להשתמש במכשירים הפרטיים שלנו לצורכי עבודה, כמו לקרוא דוא"ל ארגוני במחשב הנייד הפרטי, או לבצע שיחות והתכתבויות במדיות השונות בנושאים הקשורים לעבודה. גם במקרים אלה אתם עלולים להוות יעד לתקיפה בהיבט אישי או ארגוני.

נעלו את המכשיר באמצעות סיסמה / קוד / נעילת דפוס / אמצעי ביומטרי. הגדירו אימות דו שלבי בכל אפליקציה המאפשרת זאת.

התקינו **עדכוני תוכנה** מיד עם פרסומם. הגדירו עדכוני תוכנה אוטומטיים לכלל התוכנות במכשירכם (מומלץ להגדיר עדכונים לשעות הלילה).

הקפידו להתקין תוכנת **אנטי וירוס וחומת אש** מעודכנת.

בצעו **גיבויים** לכל מכשיריכם והמידע האגור בהם. כך, במקרה של גניבה/פריצה/איבוד מכשיר - ניתן יהיה לשחזר את המידע. מומלץ לגבות בהתקן חיצוני ו/או בענן (המספק הצפנה ו- 2FA).

הימנעו מהורדת אפליקציות ממקורות או מקישורים שאינם מוכרים. הורידו אפליקציות רק **מחנויות מורשות,** המספקות הגנה מסוימת מפני וירוסים.

מידי פעם בדקו בהגדרות המכשיר אילו הרשאות גישה אישרתם לאפליקציות השונות (מיקום, מצלמה, מיקרופון וכד'). הסירו **הרשאות מיותרות** שאינן רלוונטיות.

כסו את המצלמה במכשירכם כאשר לא נעשה בה שימוש.

בסיום השימוש במכשירכם, בצעו **התנתקות מסודרת** מכלל החשבונות. פעולה זו חשובה במיוחד בעת מסירת מכשיר לתיקון במעבדה (חשוב לפנות לשירותי מעבדה מורשית).

שימוש בהתקנים חיצוניים

טרם הכנסת קבצים שונים המגיעים מחוץ לארגון לתוך הרשת הארגונית יש לפנות לגורם האחראי בארגון לצורך בדיקתם. ניתן לבקש להעביר אליכם קבצים בדוא"ל/Gmail על מנת שיעברו סינון מסוים של הארגון.

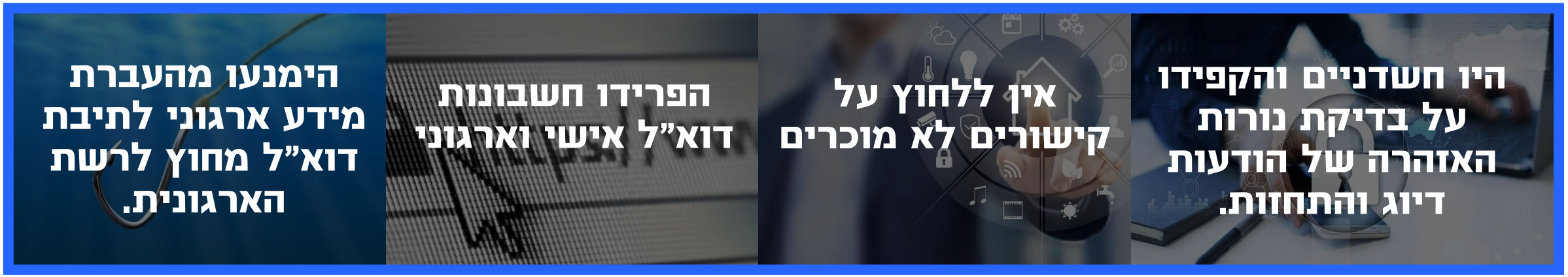
***תהליך הלבנה - ביצוע סריקה וניקוי מאיומי קוד עוין לפני הכנסת המדיה למערכות הארגון.**

סייבר ישראל
מערך הסייבר הלאומי

הגנה על דואר אלקטרוני

הגנה על דואר אלקטרוני

להקטנת הסיכון שגורם לא מורשה יוכל לקרוא התכתבויות ולפגוע במידע,
הקפידו על כללי אבטחה בסיסיים:



סייבר ישראל
מערך הסייבר הלאומי

גלישה בטוחה באינטרנט

גלישה בטוחה באינטרנט

- כתובת אתר מאובטחת ולצידה סמליל של מנעול סגור.
- עיצוב אתר בצורה לא מקצועית.
- הימנעו מלהזין פרטים רגישים.
- התאמת שם האתר לתוכנו.
- פרטי יצירת קשר/מדיניות/תקנון.

סייבר ישראל
מערך הסייבר הלאומי

רשתות חברתיות

רשתות חברתיות

בחנו את הגדרות האבטחה של האפליקציות השונות

נקטו משנה זהירות בלחיצה על קישורים או צרופות

היזהרו מפרופילים מתחזים ומזויפים

הגדירו מדיניות פרטיות וצמצמו את המידע שאתם חושפים למינימום ההכרחי

דיווח אירוע חריג

במקרה של חשד או אי ודאות, חשוב לדווח מיד לגורם האחראי בארגון

- כאשר ישנה פגיעה ודאית או חשד לפגיעה באבטחת מידע
- כאשר קיים או ישנו חשד לתקלה תפעולית, אשר עלולה לגרום לפגיעה באבטחת המידע
- כאשר יש זיהוי או חשד לפעולה חשודה של עמית או יריב
- כאשר נגנב מחשב/ציוד קצה השייך לארגון או מכשיר נייד אישי, שאפשר באמצעותו להיכנס למייל הארגוני
- הימצאות של גורם חשוד או לא מורשה במתחם הארגון

סייבר ישראל
מערך הסייבר הלאומי

למידע והמלצות נוספות
בקרו באתר מערך הסייבר הלאומי
www.cyber.gov.il

צרו קשר בטלפון 119
או בדוא"ל
119@cyber.gov.il