שם: _____ תאריך: _____ ציון: _____

# מניעת גניבת זהות ונכסים
# מדריך אבטחה

דליפות אישורי גישה, MFA, ניטור הרשת האפלה, התראות הקפאת אשראי, הנדסה חברתית

## סקירת למידה: מניעת גניבת זהות

**ברוכים הבאים!** חוברת הפעילויות הזו תדריך אתכם דרך מניעה והפחתה של גניבת זהות. תחקרו דליפות פרטי כניסה, אימות רב-גורמי, ניטור הרשת האפלה, התראות הקפאת אשראי והגנה מפני הנדסה חברתית.

**נקודות הביקורת בדף העבודה**

- ☐ **חלק 1-4: שלטו באבטחת סייבר ובמניעת איומים.**
- ☐ **חלק 5-7: פתרו תשבצים ופאזלי חיפוש מילים.**
- ☐ **חלק 8-9: פתרו מקרי בוחן ואתגר צופן.**
- ☐ **חלק 10: סקרו את דפי השאלות הנפוצות הבסיסיים והמתקדמים.**
- ☐ **חלק 11: חקרו 10 עובדות מעניינות מהעולם האמיתי.**
- ☐ **בונוס: אתגר חשבו מהר**

### אובטח
**הצפנת נתונים**
תקן AES של 256 סיביות

### תואם
**תקנים עולמיים**
מסגרות GDPR ו-CCPA

### אפס אמון
**מדיניות גישה**
אימות רב-גורמי

**פתחו את מדריך אבטחת הסייבר של VPN.com**

URL: https://www.vpn.com/cybersecurity/identity-theft/

# מפת הלמידה שלכם: הגנה על זהות

- הבינו את סיכוני חשיפת פרטי הכניסה בפורומים ברשת האפלה.
- יישמו אימות רב-גורמי (MFA) והתראות הקפאת אשראי.
- תכננו הגנות אבטחה ארגוניות מפני הונאות הנדסה חברתית ממוקדות.

### הוראות למדריך בנושא גניבת זהות

ענו על שאלות אמריקאיות ועל שאלות נכון/לא נכון, השלימו את המשפטים החסרים בעזרת בנק המילים, התאימו הגדרות ופתרו את התשבץ ואת תפזורת המילים. יישמו את הידע שלכם בנושא הגנה על זהות. ולסיום, פעילות הבונוס "חשבו מהר".

### מניעת גניבת זהות ואבטחת נכסים (מבוא)

גניבת זהות מנצלת פרטי התחברות שדלפו והתחברויות חלשות כדי לחטוף חשבונות אישיים וארגוניים. פריסת MFA, הקפאות אשראי, סורקי רשת אפלה ומסגרות SPF/DKIM/DMARC יוצרת הגנה קריטית מפני התחזות דיגיטלית.

**קראו כל נקודת ביקורת בעיון ובחרו או כתבו את התגובה הנכונה.**

# נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהי השיטה העיקרית שבה גנבי זהות גונבים פרטי התחברות?

- A. שליחת התראות אימייל מזויפות שמשכנעות משתמשים להזין סיסמאות בפורטלים מתחזים
- B. האזנה לשידורי רדיו ליד משרדו התאגידי של משתמש
- C. איחוי (דפרגמנטציה) של כונן האחסון המקומי של השרת של משתמש
- D. ניתוק תצורות גיבוי רשת חיצוניות

2. איזו בקרת אבטחה מספקת את ההגנה החזקה ביותר מפני דליפת פרטי התחברות?

- A. אימות רב-גורמי באמצעות מפתחות חומרה
- B. יצירת סיסמאות ארוכות בפורמטים ברירת מחדל של הדפדפן
- C. החלפת שמות משתמש בדוא"ל כל שישה חודשים
- D. מחיקת היסטוריות מעקב של עוגיות שמורות בדפדפן

3. מה מייצג הקפאת אשראי?

- A. נעילת דוחות אשראי כדי למנוע מגנבים לפתוח הלוואות לא מורשות
- B. מחיקת היסטוריות עסקאות של חשבונות בנק ממסדי נתונים
- C. השבתת קוראי כרטיסי אשראי מגנטיים בסורקים
- D. הצפנת כונני מסד נתונים מקומיים במצב מנוחה

4. מדוע ניטור הרשת האפלה שימושי?

- A. הוא מתריע למשתמשים אם אישורי הגישה שלהם שדלפו מופיעים במסדי נתונים לא חוקיים
- B. הוא מונע מנוזקה פעילה לפעול בארגזי חול וירטואליים
- C. הוא מאיץ את מהירויות הניתוב בדפדפן ברשתות וירטואליות
- D. הוא חוסם ניסיונות גישה של SQL injection למסד הנתונים האחורי

5. מה משמעות הנדסה חברתית?

- A. מניפולציה באנשים כדי שיחשפו מרצונם אישורי גישה חסויים
- B. סריקת פורטים בשרתים ארגוניים לאיתור ניצולי אבטחה פעילים
- C. גיבוי קובצי מסד נתונים של המערכת לכוננים קשיחים לא מקוונים
- D. ניתוב חבילות רשת דרך שלושה צמתי בצל מוצפנים

## נקודת ביקורת 2: אתגר נכון או לא נכון

**שאלה 6**

6. גניבת זהות משפיעה רק על חשבונות דיגיטליים מקוונים, ולא על דואר פיזי.

נכון  לא נכון

**שאלה 7**

7. אכיפת MFA בכל החשבונות האישיים חוסמת את רוב התקפות הבוטים של מילוי פרטי גישה.

נכון  לא נכון

**שאלה 8**

8. הקפאת אשראי חוסמת בדיקות אשראי אך מונעת ממך גישה לחשבון הבנק שלך.

נכון  לא נכון

**שאלה 9**

9. מנהלי סיסמאות מגנים על משתמשים מפני פישינג בכך שהם מסרבים למלא סיסמאות אוטומטית בדומיינים מזויפים.

נכון  לא נכון

**שאלה 10**

10. הודעות דוא"ל של פישינג משתמשות לעיתים קרובות בלשון דחופה כדי לעורר תגובות רגשיות ומהירות.

נכון  לא נכון

# נקודת ביקורת 3: השלמת מונחי מפתח

קראו כל משפט שלהלן והשלימו את החסר במונח הנכון מבנק המילים.

1. גנבי זהות מכוונים אל סיסמאות אישיות ואל _____ של המשתמשים.
2. התראה למשתמשים על פריצות למסדי נתונים מזהה _____ של חשבונות פרטיים.
3. דרישה לקוד זמני כדי להיכנס נקראת _____ .
4. סריקת פורומים של האקרים לאיתור נתונים גנובים היא _____ של הרשת האפלה.
5. חסימת בדיקות אשראי לא מורשות מחייבת _____ אשראי.
6. הדרכת עובדים במודעות לפישינג בונה קו _____ פעיל בתחום האבטחה.

**בנק מילים**

אימות רב-גורמי | אישורים | דליפות | הגנה | הקפאה | זיוף | ניטור | פישינג

**כתבו את תשובותיכם כאן:**

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

# נקודת ביקורת 4: התאמת מושגים באבטחה

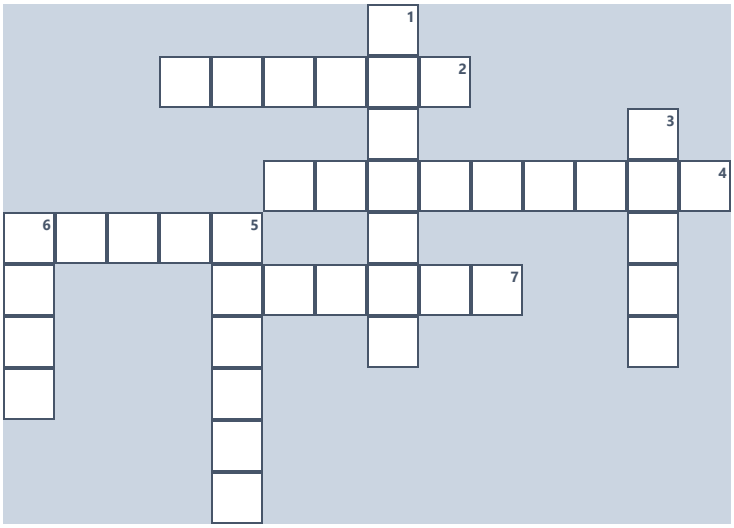
**התאמת הגדרות**

התאימו כל מונח אוצר מילים בצד ימין להגדרה הנכונה שלו בצד שמאל על ידי כתיבת האות המתאימה (A-H) בתיבת הקלט הניתנת למילוי.

| | | |
|---|---|---|
| 1. אישורי גישה | A | שלב אימות משני (כגון מפתחות חומרה) המגן על כניסות לחשבון. |
| 2. דליפות | B | יצירת אתר או הודעת דוא"ל מזויפים כדי לחקות ארגון לגיטימי. |
| 3. MFA | C | הגבלת גישה לתיקי אשראי כדי למנוע בקשות הלוואה מזויפות. |
| 4. ניטור | D | חשיפה לא מורשית של מסדי נתונים פרטיים המכילים רשומות משתמשים אישיות. |
| 5. הקפאה | E | הדרכה ובקרות טכניות המשמשות להגנה מפני גניבת זהות. |
| 6. הגנה | F | שליחת הודעות הונאה כדי להערים על משתמשים למסור פרטי גישה. |
| 7. זיוף | G | סריקת פורומים מקוונים וערוצי האקרים לאיתור נתונים ארגוניים גנובים. |
| 8. פישינג | H | שמות משתמש, סיסמאות ואסימונים פרטיים המשמשים לאימות זהויות דיגיטליות. |

# נקודת ביקורת 5: תשבץ

פתרו את התשבץ על ידי הקלדת אותיות בתיבות הלבנות הפעילות. המספרים מתאימים לרמזים שלהלן.




## מאוזן

**2. שליחת הודעות מתעתעות כדי לגרום למשתמשים למסור אישורי כניסה (6)**

**4. שלב אימות שני (כגון מפתחות חומרה) המגן על כניסות לחשבון (9)**

**5. הגבלת הגישה לתיקי אשראי כדי למנוע בקשות הלוואה במרמה (5)**

**7. חשיפה בלתי מורשית של מסדי נתונים פרטיים המכילים רשומות אישיות של משתמשים (6)**

## מאונך

**1. שמות משתמש, סיסמאות ואסימונים פרטיים המשמשים לאימות זהויות דיגיטליות (7)**

**3. סריקת פורומים וערוצי האקרים לאיתור נתונים ארגוניים גנובים (5)**

**5. יצירת אתר או דוא"ל מזויפים המחקים ארגון לגיטימי (6)**

**6. הדרכה ובקרות טכניות המשמשות לשמירה מפני גניבת זהות (4)**

# נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

משתמשי קורא מסך ומקלדת יכולים להקליד את תשובות התשבץ ישירות בשדות הטקסט שלהלן.

## מאוזן

**2 מאוזן: שליחת הודעות מתעתעות כדי לגרום למשתמשים למסור אישורי כניסה (6 אותיות):**

**4 מאוזן: שלב אימות שני (כגון מפתחות חומרה) המגן על כניסות לחשבון (9 אותיות):**

**5 מאוזן: הגבלת הגישה לתיקי אשראי כדי למנוע בקשות הלוואה במרמה (5 אותיות):**

**7 מאוזן: חשיפה בלתי מורשית של מסדי נתונים פרטיים המכילים רשומות אישיות של משתמשים (6 אותיות):**

## מאונך

**1 מאונך: שמות משתמש, סיסמאות ואסימונים פרטיים המשמשים לאימות זהויות דיגיטליות (7 אותיות):**

**3 מאונך: סריקת פורומים וערוצי האקרים לאיתור נתונים ארגוניים גנובים (5 אותיות):**

**5 מאונך: יצירת אתר או דוא"ל מזויפים המחקים ארגון לגיטימי (6 אותיות):**

**6 מאונך: הדרכה ובקרות טכניות המשמשות לשמירה מפני גניבת זהות (4 אותיות):**

# נקודת ביקורת 6: חיפוש מילה נסתרת

מצאו את 8 מונחי המפתח בלוח שלהלן. מילים יכולות להופיע אופקית, אנכית או באלכסון.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| י | ת | ת | ל | ף | ס | ת | נ | ו | ס | כ | ג | פ | ח | ו |
| מ | ו | ע | ל | ס | ת | ע | י | פ | נ | ג | ק | צ | צ | ה |
| כ | פ | ה | ט | ב | א | ב | ט | ג | י | נ | ם | כ | י | ם |
| כ | י | נ | ת | ק | י | ד | ו | ע | ל | ש | ט | ד | ח | מ |
| מ | ל | ג | י | ע | א | ס | ר | ז | ל | ה | י | ל | ע | פ |
| צ | ד | ה | ק | ק | י | ז | א | ג | צ | ס | ק | נ | נ | ח |
| ת | פ | ב | ש | ד | מ | צ | ף | י | ר | ג | ף | פ | ג | ש |
| ו | ו | י | ז | ף | ו | ד | מ | ד | ש | ע | ת | ס | א | ג |
| ז | ק | ב | א | ף | ת | מ | ד | כ | א | ו | ד | נ | ד | ה |
| ח | ה | ז | ח | ד | נ | פ | ע | ל | ה | ח | ר | פ | ף | צ |
| ת | ה | ע | ר | ה | ו | א | א | ע | נ | מ | ס | י | ק | ת |
| ה | ע | י | פ | ק | ס | פ | ג | מ | ם | ב | ו | פ | ם | ת |
| ש | ט | א | פ | ף | ף | ם | ם | כ | ו | ח | ל | ע | י | ל |
| ל | צ | נ | ז | ס | ע | ז | ף | א | נ | ר | ו | ר | ב | ם |
| פ | ם | ב | ז | ל | ף | ז | י | נ | ס | מ | ת | ג | ל | ף |

**רשימת מילים**

אישורים | דליפות | אימותנוסף | ניטור | הקפאה | הגנה | התחזות | פישינג

# נקודת ביקורת 6 – פעילות חלופית: התאמת אוצר מילים נגישה

התאימו כל אחד מ-8 מונחי המילון מתפזורת המילים להגדרה הנכונה שלו על ידי כתיבת האות (A-H) במקום הריק.

| מונחי אוצר מילים |
|---|
| **A. אישורים** |
| **B. דליפות** |
| **C. אימותנוסף** |
| **D. ניטור** |
| **E. הקפאה** |
| **F. הגנה** |
| **G. התחזות** |
| **H. פישינג** |

| | הגדרות ושדות התאמה |
|---|---|
| | 1. שליחת הודעות מתעתעות כדי לגרום למשתמשים למסור אישורי כניסה. |
| | 2. שמות משתמש, סיסמאות ואסימונים פרטיים המשמשים לאימות זהויות דיגיטליות. |
| | 3. יצירת אתר או דוא"ל מזויפים המחקים ארגון לגיטימי. |
| | 4. הדרכה ובקרות טכניות המשמשות לשמירה מפני גניבת זהות. |
| | 5. סריקת פורומים וערוצי האקרים לאיתור נתונים ארגוניים גנובים. |
| | 6. הגבלת הגישה לתיקי אשראי כדי למנוע בקשות הלוואה במרמה. |
| | 7. חשיפה בלתי מורשית של מסדי נתונים פרטיים המכילים רשומות אישיות של משתמשים. |
| | 8. שלב אימות שני (כגון מפתחות חומרה) המגן על כניסות לחשבון. |

## נקודת ביקורת 7: אתגר מילים מבולבלות

סדרו מחדש את האותיות שלהלן כדי לחשוף מושגים ומונחים מרכזיים באבטחת סייבר. כתבו את תשובותיכם בתיבות הקלט המסופקות.

1. ויארמשי
2. ךאסוינותמ
3. פההאק
4. תזחוהת
5. פיתדול
6. ונטרי
7. נההג
8. שגפניי

# פעילות בונוס: חשבו מהר

כתבו 3 תשובות לכל קטגוריה. מי שמסיים ראשון את הרשימה מנצח.

| | | | |
|---|---|---|---|
| 1 | דברים שעושים אם זהותכם נגנבה | | |
| 2 | דברים שאין לשתף ברשתות החברתיות | | |
| 3 | דברים שמגבים | | |
| 4 | כרטיסים או תעודות בארנק שלכם | | |
| 5 | מסמכים שכדאי להגן עליהם | | |
| 6 | דברים שעושים אחרי דליפת נתונים | | |
| 7 | סיבות לעדכן תוכנה | | |
| 8 | מידע שגנב זהויות רוצה | | |
| 9 | מכשירים שאפשר לפרוץ אליהם | | |
| 10 | מקומות שמהם הנתונים שלכם יכולים לדלוף | | |
| 11 | הרגלים בטוחים שאפשר להתחיל כבר היום | | |
| 12 | סימנים לכך שמחשב נדבק | | |
| 13 | דרכים להוכיח מי אתם | | |
| 14 | סימנים לגניבת זהות | | |
| 15 | סימני אזהרה באימייל | | |

# נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

יישמו את המושגים שלמדתם כדי לפתור את התרחישים מהעולם האמיתי שלהלן.

### מקרה בוחן 1: הגנה מפני התחזות לזהות של מנהלים

👨‍💻

**תרחיש:** מנהל בכיר ברמת C-suite בעל פרופיל גבוה הפך ליעד של שמות דומיין שמנצלים שגיאות הקלדה (typosquatting) ומחקים את האימייל האישי שלו כדי להונות לקוחות. תכננו תוכנית להגנת מותג.

**שאלה לדיון:** נתחו את סיכוני התחזות למותג, ופרטו את בקרות SPF/DKIM/DMARC והאימות.

### מקרה בוחן 2: חשיפת אישורי גישה ארגוניים ברשת האפלה

👨‍💻

**תרחיש:** ממאגר נתונים שדלף ופורסם ברשת האפלה (dark web) מכיל כמה מאות פרטי גישה ארגוניים השייכים למנהלי מערכת של ארגון. תכננו אסטרטגיית הפחתת סיכונים.

**שאלה לדיון:** תארו בקצרה את תהליך ניקוי פרטי הגישה, ותכננו פריסה של מנהל סיסמאות.

# נקודת ביקורת 9: פענוח הצופן

איש מקצוע באבטחת סייבר מגן על נכסי רשת מפני גורמי איום מקוונים. השתמשו במפתח האותיות-למספרים שלהלן כדי לפענח את ההודעה, וכתבו את האותיות המתאימות במקומות הריקים.

**מפתח הצפנה של אות למספר**

**א=1 ב=2 ג=3 ד=4 ה=5 ו=6 ז=7 ח=8 ט=9**

**י=10 כ=11 ל=12 מ=13 נ=14 ס=15 ע=16 פ=17 צ=18**

**ק=19 ר=20 ש=21 ת=22 ך=23 ם=24 ן=25 ף=26 ץ=27**

| 22 | 6 | 13 | 10 | 1 | 2 | | 24 | 11 | 22 | 6 | 5 | 7 | | 12 | 16 | | 6 | 14 | 3 | 5 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | |

| 24 | 10 | 13 | 20 | 6 | 3 | | 5 | 2 | 6 | 20 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

**ההודעה המפוענחת:**

**טיפ: כל מספר מייצג אות עברית אחת מהמפתח שלמעלה.**

# נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק A)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

**Q1: מהי גניבת זהות?**

פשע שבו תוקף גונב רשומות אישיות (כמו סיסמאות או מספרי ביטוח לאומי) כדי להתחזות לאדם אחר לצורך רווח כספי.

**Q2: מהי הסיבה הנפוצה ביותר לגניבת זהות?**

פישינג הוא אחת הדרכים המובילות שבהן גנבים משיגים סיסמאות, והוא מפתה משתמשים לאתרים מזויפים ומתחזים.

**Q3: כיצד אימות רב-שלבי (MFA) מגן על זהויות?**

MFA דורש הוכחה שנייה (כמו מפתח חומרה) כדי להתחבר, וחוסם תוקפים גם אם גנבו את הסיסמה שלכם.

**Q4: מהי הקפאת אשראי?**

שירות חינמי שחוסם סוכנויות אשראי משיתוף קובץ האשראי שלך, ועוצר גנבים מלפתוח הלוואות חדשות על שמך. [2]

**Q5: מהו ניטור הרשת האפלה (dark web monitoring)?**

תוכנה הבודקת בפורומים של האקרים אם דלפו כתובות דוא״ל, סיסמאות ורשומות אישיות, ומתריעה אם הנתונים שלכם נחשפו.

# נקודת ביקורת 10: שאלות נפוצות על אבטחת סייבר – בסיסי (חלק B)

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

**Q6: מה משמעות credential stuffing?**

בוטים אוטומטיים הבודקים רשימות סיסמאות שדלפו במאות אתרים כדי להשתלט על חשבונות פעילים.

**Q7: מדוע זיוף אימייל מסוכן?**

הוא מאפשר לתוקפים לזייף את שם השולח בהודעות דוא"ל, כך שהודעות פישינג ייראו כאילו הגיעו מעמיתים מהימנים.

**Q8: כיצד מנהלי סיסמאות עוצרים גניבת זהות?**

הם מאחסנים סיסמאות מורכבות וייחודיות לכל חשבון ומסרבים למלא אוטומטית פרטי כניסה בדומיינים מזויפים של פישינג.

**Q9: מהו spear phishing?**

התקפת פישינג ממוקדת מאוד שמותאמת לשם ולפרטים של הקורבן כדי להגדיל את הסיכוי להונאה.

**Q10: במה התראת אשראי שונה מהקפאה?**

התראה מורה לגורמי מימון לאמת את זהותך לפני פתיחת חשבונות, ואילו הקפאה חוסמת לחלוטין גישה לקובץ האשראי שלך. [2]

# נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק C)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

### Q1: כיצד החלפת SIM מובילה לגניבת זהות?

תוקפים משכנעים את צוות חברת הסלולר להעביר את מספר הטלפון של הקורבן לכרטיס SIM חדש, וכך חוטפים קודי 2FA הנשלחים ב-SMS.

### Q2: מהו תפקידו של DMARC במניעת גניבת זהות?

DMARC מאפשר לבעלי דומיינים לחסום הודעות דוא״ל מזויפות מלהגיע לתיבות הדואר, ובכך מונע דוא״ל מזויף שמתחזה לדומיינים של ארגונים.

### Q3: מדוע קשה לזהות גניבת זהות סינתטית?

גנבים משלבים מספרי ביטוח לאומי אמיתיים עם שמות ותאריכי לידה מזויפים כדי לבנות פרופילי אשראי חדשים לגמרי, ועוקפים התראות הונאה בסיסיות.

### Q4: כיצד מתווכי נתונים מנצלים זהויות אישיות?

מתווכי נתונים (data brokers) אוספים רשומות ציבוריות, התנהגות ברשת והיסטוריות רכישה כדי לבנות תיקי פרופיל, שעלולים לדלוף או להימכר.

### Q5: מדוע MFA מבוסס SMS נחשב פגיע?

תעבורת SMS פגיעה ליירוט, לפישינג ולניצולי החלפת SIM ברמת חברת הסלולר.

# נקודת ביקורת 10: שאלות נפוצות על אבטחה – מתקדם (חלק D)

חקרו היבטים טכניים מתקדמים של מסגרות אבטחה, ניתוח נוזקות ועמידה בדרישות נתונים.

### Q6: מהי נעילת קובץ אשראי?

שירות מסחרי הדומה להקפאה, שמאפשר למשתמשים לפתוח או לנעול מיד את תיק האשראי שלהם דרך אפליקציה לנייד.

### Q7: כיצד פריצות לנתוני חברות מזינות גניבת זהות?

מסדי נתונים שדלפו חושפים מיליוני פרטי גישה גלויים, ומספקים לגנבים את הנתונים הגולמיים הדרושים לביצוע הונאת זהות ממוקדת.

### Q8: מהו הסיכון בשיתוף יתר ברשתות חברתיות?

שיתוף פומבי של שמות חיות מחמד, מקומות לידה ושמות נעורים של אמהות מספק לגנבים את התשובות לשאלות נפוצות לשחזור חשבון.

### Q9: כיצד התחברות ביומטרית מגינה על פרופילי זהות?

ביומטריה קושרת התחברויות למאפיינים כמו טביעות אצבע או פנים; כשהיא נשמרת במכשיר קשה לגנוב אותה, אך נתונים ביומטריים מאוחסנים עלולים לדלוף.

### Q10: כיצד כלל Red Flags נלחם בגניבת זהות?

תקנה פדרלית שמחייבת מוסדות פיננסיים לפתח תוכניות כתובות לזיהוי סימני אזהרה לגניבת זהות ולהגיב אליהם.

# חלק 11: 10 עובדות ותובנות מהעולם האמיתי על אבטחת סייבר

עיינו בעובדות מהעולם האמיתי על פריצות אבטחה, מנגנוני הגנה ותקני ציות.

### 1. תובנות על אבטחה

IdentityTheft.gov, שמופעל על ידי ה-FTC, מאפשר לקורבנות בארה"ב לדווח על גניבת זהות ולקבל תוכנית התאוששות אישית. [1]

### 2. תובנות על אבטחה

מפתחות אבטחה בחומרה הם MFA עמיד בפני פישינג, סוג ה-MFA החזק ביותר ש-CISA ממליצה עליו. [4]

### 3. תובנות על אבטחה

סיסמאות שנפגעו הן נקודת כניסה נפוצה בפרצות נתונים, ומזינות הונאות זהות מאוחרות יותר.

### 4. תובנות על אבטחה

הקפאת אשראי היא חינמית לפי החוק הפדרלי, ומונעת מגורמי מימון לבדוק קבצי אשראי עד לפתיחתה. [2]

### 5. תובנות על אבטחה

DMARC מאפשר לבעלי דומיינים להורות לשרתי דואר לדחות או להעביר להסגר דוא"ל מזויף שנכשל בבדיקות. [7]

### 6. תובנות על אבטחה

החלפת SIM (SIM swapping) מאפשרת להאקרים לעקוף אימות דו-שלבי מבוסס SMS בפורטלי בנקאות.

### 7. תובנה על אבטחה

הונאת זהות סינתטית מערבבת פרטים אמיתיים ובדויים, ולכן קשה למלווים לזהותה.

### 8. תובנה על אבטחה

אנשים רבים משתמשים באותה סיסמה בכמה חשבונות מקוונים, ולכן פריצה אחת עלולה לחשוף כמה מהם.

### 9. תובנה על אבטחה

ברוקרי נתונים אוספים תיקים מפורטים על מספר רב של צרכנים, מה שיוצר סיכון פרטיות מרוכז.

### 10. תובנות על אבטחה

התאוששות מגניבת זהות יכולה לדרוש חודשים של עבודה, כמו ערעור על חיובים ותיקון דוחות אשראי.

# מקורות והפניות טכניים

מדריך הלימוד והפאזלים האינטראקטיביים נערכו על סמך תקנים גלובליים של NIST, OWASP ותאימות לפרטיות נתונים.

## מקורות אקדמיים ותעשייתיים

[1] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.
https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.
https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.
https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).
https://www.rfc-editor.org/rfc/rfc7489.html

## מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

**1 שאלה 1** — **תשובה נכונה: A**

### הערה למורה

מהי השיטה העיקרית שבה גנבי זהות גונבים פרטי התחברות? → שליחת התראות אימייל מזויפות שמשכנעות משתמשים להזין סיסמאות בפורטלים מתחזים

**2 שאלה 2** — **תשובה נכונה: A**

### הערה למורה

איזו בקרת אבטחה מספקת את ההגנה החזקה ביותר מפני דליפת פרטי התחברות? → אימות רב-גורמי באמצעות מפתחות חומרה

**3 שאלה 3** — **תשובה נכונה: A**

### הערה למורה

מה מייצג הקפאת אשראי? → נעילת דוחות אשראי כדי למנוע מגנבים לפתוח הלוואות לא מורשות

**4 שאלה 4** — **תשובה נכונה: A**

### הערה למורה

מדוע ניטור הרשת האפלה שימושי? → הוא מתריע למשתמשים אם אישורי הגישה שלהם שדלפו מופיעים במסדי נתונים לא חוקיים

**5 שאלה 5** — **תשובה נכונה: A**

### הערה למורה

מה משמעות הנדסה חברתית? → מניפולציה באנשים כדי שיחשפו מרצונם אישורי גישה חסויים

## מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

**6** **שאלה 6**

תשובה נכונה: לא נכון

### הערה למורה

גניבת זהות יכולה להתחיל גם לא מקוון, למשל מדואר או ממסמכים גנובים.

**7** **שאלה 7**

תשובה נכונה: נכון

### הערה למורה

אכיפת MFA בכל החשבונות האישיים חוסמת את רוב התקפות הבוטים של מילוי פרטי גישה.

**8** **שאלה 8**

תשובה נכונה: לא נכון

### הערה למורה

הקפאת אשראי עוצרת בדיקות אשראי חדשות אך אינה משפיעה על החשבונות הקיימים שלכם.

**9** **שאלה 9**

תשובה נכונה: נכון

### הערה למורה

מנהלי סיסמאות מגנים על משתמשים מפני פישינג בכך שהם מסרבים למלא סיסמאות אוטומטית בדומיינים מזויפים.

**10** **שאלה 10**

תשובה נכונה: נכון

### הערה למורה

הודעות דוא"ל של פישינג משתמשות לעיתים קרובות בלשון דחופה כדי לעורר תגובות רגשיות ומהירות.

# מפתחות אוצר מילים ומחוון הערכה

**מחוון הערכה למורה: תנו 1 נקודה לכל התאמה נכונה (סה"כ 8 נקודות) ולכל מונח הקשר (סה"כ 6 נקודות).**

## נקודת ביקורת 4: מפתח תשובות – התאמת מושגים

| | | | |
|---|---|---|---|
| H 1. אישורי גישה | D 2. דליפות | A 3. MFA | G 4. ניטור |
| C 5. הקפאה | E 6. הגנה | B 7. זיוף | F 8. פישינג |

## נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

| | | | |
|---|---|---|---|
| 1 אישורים | 2 דליפות | 3 אימות רב-גורמי | 4 ניטור |
| 5 הקפאה | 6 הגנה | | |

## נקודת ביקורת 6 – פעילות חלופית: מפתח תשובות – התאמת אוצר מילים

| | | | |
|---|---|---|---|
| 1 H – פישינג | 2 A – אישורים | 3 G – התחזות | 4 F – הגנה |
| 5 D – ניטור | 6 E – הקפאה | 7 B – דליפות | 8 C – אימותנוסף |

### הערות לדיון עבור מורים

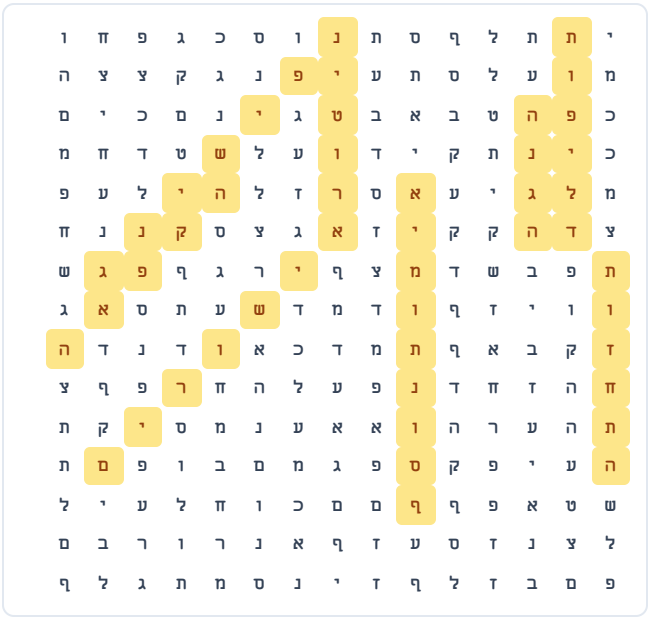
**מונחי מפתח:**
ודאו שהתלמידים מסבירים במילים שלהם את אישורי גישה, דליפות ו-MFA ונותנים דוגמה לכל אחד מהם.

**מקרי בוחן:**
בקשו מהתלמידים לבסס את ההמלצות שלהם על עובדות מדף העבודה ולא על דעות.

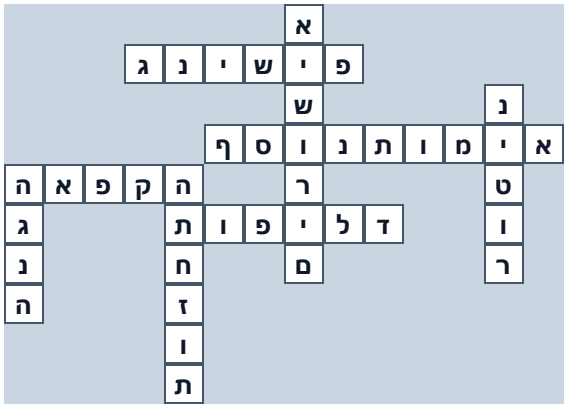
**הערכת מקורות:**
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

# מפתחות פאזלים והערות למורה

## פתרון תפזורת



## פתרון תשבץ



## מדריך למורה לפתרונות התשבץ

### מאוזן

**2 מאוזן: פישינג** שליחת הודעות מתעתעות כדי לגרום למשתמשים למסור אישורי כניסה (6 אותיות)

**4 מאוזן: אימותנוסף** שלב אימות שני (כגון מפתחות חומרה) המגן על כניסות לחשבון (9 אותיות)

**5 מאוזן: הקפאה** הגבלת הגישה לתיקי אשראי כדי למנוע בקשות הלוואה במרמה (5 אותיות)

**7 מאוזן: דליפות** חשיפה בלתי מורשית של מסדי נתונים פרטיים המכילים רשומות אישיות של משתמשים (6 אותיות)

### מאונך

**1 מאונך: אישורים** שמות משתמש, סיסמאות ואסימונים פרטיים המשמשים לאימות זהויות דיגיטליות (7 אותיות)

**3 מאונך: ניטור** סריקת פורומים וערוצי האקרים לאיתור נתונים ארגוניים גנובים (5 אותיות)

**5 מאונך: התחזות** יצירת אתר או דוא"ל מזויפים המחקים ארגון לגיטימי (6 אותיות)

**6 מאונך: הגנה** הדרכה ובקרות טכניות המשמשות לשמירה מפני גניבת זהות (4 אותיות)

# מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

### מפתח פענוח מילים מבולבלות

1. ויארשי — **אישורים**
2. ךאסוינותמ — **אימותנוסף**
3. פההאק — **הקפאה**
4. תזחוהת — **התחזות**
5. פיתדול — **דליפות**
6. ונטרי — **ניטור**
7. נההג — **הגנה**
8. שגפניי — **פישינג**

### מפתח אתגר הצופן הסודי

**"הגנו על זהותכם באימות מרובה גורמים"**

# מפתח תשובות למקרי הבוחן

## A מקרה בוחן 1: הגנה מפני התחזות לזהות של מנהלים

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מנהל בכיר בעל פרופיל גבוה (C-suite) הפך ליעד של דומיינים מזויפים בשגיאות הקלדה (typosquatting) שמחקים את הדוא"ל האישי שלו כדי להונות לקוחות. תכננו תוכנית להגנת מותג.
- אסטרטגיה ופתרון מומלצים: רשמו את כל גרסאות האיות הנפוצות של שם המנהל. פרסו פרוטוקולי אימות דוא"ל (DMARC, DKIM, SPF) למניעת זיוף דומיינים. אכפו MFA חומרתי בכל ההתחברויות הארגוניות של בכירי ההנהלה (C-suite).

## B מקרה בוחן 2: חשיפת אישורי גישה ארגוניים ברשת האפלה

פתרון למורה

### הנחיות הערכה

### תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: קובץ dump של מסד נתונים מהרשת האפלה מכיל כמה מאות פרטי התחברות ארגוניים השייכים למנהלי מערכת של ארגון. תכננו אסטרטגיית צמצום.
- אסטרטגיה ופתרון מומלצים: בצעו איפוס סיסמאות בכל החברה. הורו על שימוש במנהל סיסמאות ארגוני. אכפו MFA בכל פורטלי המערכת והגדירו התראות אוטומטיות רציפות לניטור הרשת האפלה.