שם: _____ תאריך: _____ ציון: _____

הונאות מקוונות והנדסה חברתית מדריך הגנה

פישינג בדוא"ל, דומיינים מזויפים, ויישינג, הונאות תמיכה, אימות חוץ-תחומי, BEC

סקירת למידה: הונאות מקוונות

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך הגנה מפני הונאות מקוונות. תחקרו אתרי פישינג מזויפים, טקטיקות הנדסה חברתית, הונאות תמיכה, וקטורי הונאת העברות בנקאיות ושיטות אימות תשלום.

אובטח

הצפנת נתונים

תקן AES של 256 סיביות

תואם

תקנים עולמיים

מסגרות GDPR ו-CCPA

אפס אמון

מדיניות גישה

אימות רב-גורמי

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**

פתחו את מדריך אבטחת הסייבר של VPN.com

URL: https://www.vpn.com/cybersecurity/online-scams/

מפת הלמידה שלכם: הגנה מפני הונאות מקוונות

- זהו אינדיקטורים נפוצים לתרמיות תמיכה ולדומיינים של typosquatting.
- יישמו פרוטוקולי אימות דוא״ל (SPF, DKIM, DMARC) נגד התחזות.
- הגדירו אימות עסקאות חוץ-תחומי כדי למנוע הונאות בהעברות כספים עסקיות.

הוראות למדריך הונאות מקוונות

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 מפני הונאות ברשת. ולסיום, פעילות הבונוס "חשבו מהר".

הגנה מפני הונאות מקוונות והנדסה חברתית (מבוא)

הונאות מקוונות מנצלות התנהגות אנושית באמצעות פישינג, חלונות קופצים של תמיכה, ויישינג והונאות העברה בנקאית. אכיפת אימות עסקאות בערוץ נפרד וכללי דומיין SPF/DKIM/DMARC מסייעת לחסום וקטורים של הנדסה חברתית בשער הכניסה.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו האינדיקטור העיקרי להונאת תמיכה?

- A. חלון קופץ שטוען שהמערכת שלך נגועה ודורש ממך להתקשר למספר טלפון
- B. עדכון אבטחה אוטומטי שהורד ממאגר רשמי
- C. מנהל סיסמאות המסרב למלא פרטי גישה בדומיין ארגוני
- D. גיבוי קבצים ברקע המתבצע בתצורת כונן חיצוני

2. איזו טכניקה משתמשת בדומייני שולח מזויפים כדי לגנוב פרטי בנק?

- A. פישינג באימייל
- B. סריקת פורטים
- C. הזרקת זיכרון
- D. מחיקה קריפטוגרפית

3. מה מייצג הונאת העברה בנקאית?

- A. הונאת קורבנות כדי שישלחו כסף לחשבונות ארגוניים מזויפים באמצעות הנדסה חברתית
- B. הצפנת מסדי נתונים של מערכת באמצעות מטענים של כופרה
- C. שאילתות למסדי נתונים באמצעות פקודות SQL injection
- D. גיבוי קבצי מערכת לדיסקי אחסון לא מקוונים

4. מדוע נוכלים יוצרים אתרי קניות מזויפים?

- A. כדי לגנוב פרטי כרטיס אשראי ופרטי תשלום מקונים
- B. כדי לארח טבלאות מסד נתונים לניתוח נוזקות בארגז חול
- C. כדי להאיץ את אספקת ההזמנות המקוונות
- D. כדי לבדוק עיצובי אתרים חדשים בחינם

5. מה משמעות וישינג?

- A. הונאות פישינג קולי ברשתות טלפון כדי לגנוב אישורי גישה
- B. סריקת רשתות מקומיות לאיתור מכשירים לא מאובטחים
- C. שחזור מסדי נתונים של המערכת לאחר פריצה לא מורשית
- D. הרצת קוד לא מהימן בתוך קונטיינרים וירטואליים מאובטחים

נקודת ביקורת 2: אתגר נכון או לא נכון

6 שאלה 6

6. הונאות פישינג מכוונות רק למשתמשי קצה, ולעולם לא ליעדי ציד לווייתנים בהנהלה.

נכון לא נכון

7 שאלה 7

7. דומיינים מתחזים משתמשים לעיתים קרובות בשגיאות הקלדה קלות (כמו amaz0n.com) כדי לחקות מותגים מהימנים.

נכון לא נכון

8 שאלה 8

8. ניתן לפתור הונאות תמיכה על ידי מתן גישה מרחוק למתקשר.

נכון לא נכון

9 שאלה 9

9. הנדסה חברתית מנצלת פסיכולוגיה אנושית כמו פחד ודחיפות כדי לעקוף כללי אבטחה.

נכון לא נכון

10 שאלה 10

10. יש לאמת בקשות להעברה בנקאית תמיד באמצעות ערוצי תקשורת נפרדים (out-of-band).

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מיילים מתעתעים הגורמים למשתמשים לטעות נקראים _____ .
2. כתובות אינטרנט המחקות מותגים מהימנים הן כתובות _____ .
3. הונאות קוליות המכוונות לפרטי בנק נקראות _____ .
4. חלון קופץ הדורש כסף עבור הסרת וירוס הוא מקרה של _____ בתחום התמיכה.
5. אישור בקשת תשלום מחייב _____ בערוץ נפרד.
6. הפניית עסקאות עסקיות לחשבונות גנבים היא _____ של כספים.

בנק מילים

אימות | הונאה | הסטה | וישינג | לווייתנים | מזויפות | סמישינג | פישינג

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

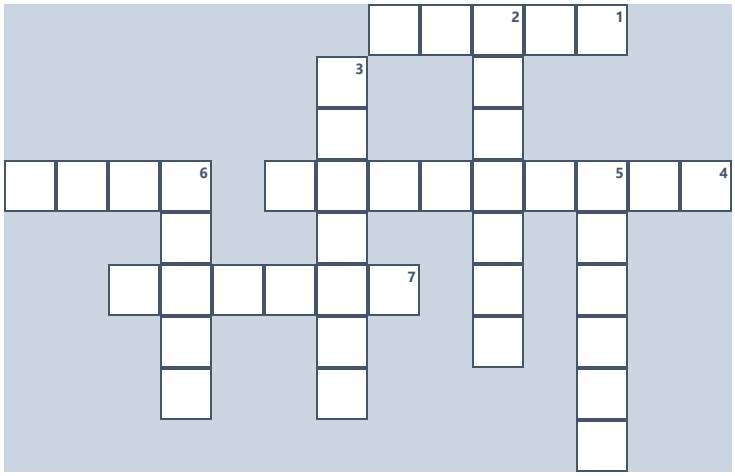
התאמת הגדרות

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

1. פישינג	A	הפניה הונאתית של עסקאות בנק לחשבונות של פושעים.
2. מזויף	B	תרמית שנועדה לגנוב כסף או פרטי גישה מקורבנות.
3. וישינג	C	שליחת הודעות טקסט הונאה כדי לגנוב פרטי גישה לחשבונות סלולריים.
4. הונאה	D	שיחות קוליות מתחזות שנועדו לגנוב פרטי התחברות ופרטי חשבון.
5. אימות	E	מתקפות פישינג ממוקדות שמטרתן לגנוב פרטי גישה ממנהלים בכירים בדרג C-level.
6. העברה בנקאית	F	כתובת שולח מייל או אתר מחקה, שנועדה להיראות לגיטימית.
7. ווישינג	G	קמפיינים של הודעות דוא"ל מתחזות שנועדו לגנוב פרטי התחברות וסיסמאות.
8. פישינג ב-SMS	H	אישור פרטי התשלום באמצעות ערוץ קשר משני מהימן.

נקודת ביקורת 5: תשבץ

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



מאוזן

1. אישור פרטי תשלום באמצעות שיטת קשר משנית מהימנה (5)

4. התקפות פישינג ממוקדות שנועדו לגנוב אישורי כניסה ממנהלים בכירים (9)

6. הפניה במרמה של עסקאות בנקאיות לחשבונות פושעים (4)

7. קמפיינים הונאתיים בדוא"ל שנועדו לגנוב אישורי כניסה וסיסמאות (6)

מאונך

2. כתובת שולח דוא"ל או אתר המדומים להיראות לגיטימיים (7)

3. שליחת הודעות טקסט הונאתיות לגניבת אישורי חשבון נייד (7)

5. שיחות קוליות הונאתיות שנועדו לגנוב אישורי כניסה ופרטי חשבון (6)

6. תכסיס מרמה שנועד לגנוב כסף או גישה לאישורים מקורבנות (5)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

1 מאוזן: אישור פרטי תשלום באמצעות שיטת קשר משנית מהימנה (5 אותיות):

4 מאוזן: התקפות פישינג ממוקדות שנועדו לגנוב אישורי כניסה ממנהלים בכירים (9 אותיות):

6 מאוזן: הפניה במרמה של עסקאות בנקאיות לחשבונות פושעים (4 אותיות):

7 מאוזן: קמפיינים הונאתיים בדוא״ל שנועדו לגנוב אישורי כניסה וסיסמאות (6 אותיות):

מאונך

2 מאונך: כתובת שולח דוא״ל או אתר המדומים להיראות לגיטימיים (7 אותיות):

3 מאונך: שליחת הודעות טקסט הונאתיות לגניבת אישורי חשבון נייד (7 אותיות):

5 מאונך: שיחות קוליות הונאתיות שנועדו לגנוב אישורי כניסה ופרטי חשבון (6 אותיות):

6 מאונך: תכסיס מרמה שנועד לגנוב כסף או גישה לאישורים מקורבנות (5 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

פישינג | מזויפות | וישינג | הונאה | אימות | הסטה | לווייתנים | סמישינג

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. פישינג
B. מזויפות
C. וישינג
D. הונאה
E. אימות
F. הסטה
G. לווייתנים
H. סמישינג

הגדרות ושדות התאמה	
1. כתובת שולח דוא״ל או אתר המדומים להיראות לגיטימיים.	
2. אישור פרטי תשלום באמצעות שיטת קשר משנית מהימנה.	
3. הפניה במרמה של עסקאות בנקאיות לחשבונות פושעים.	
4. שליחת הודעות טקסט הונאתיות לגניבת אישורי חשבון נייד.	
5. התקפות פישינג ממוקדות שנועדו לגנוב אישורי כניסה ממנהלים בכירים.	
6. שיחות קוליות הונאתיות שנועדו לגנוב אישורי כניסה ופרטי חשבון.	
7. קמפיינים הונאתיים בדוא״ל שנועדו לגנוב אישורי כניסה וסיסמאות.	
8. תכסיס מרמה שנועד לגנוב כסף או גישה לאישורים מקורבנות.	

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. שפינגי
2. גושניי
3. מאתוי
4. ימייניתלוו
5. פתיומוז
6. אהנהו
7. טההס
8. משגסניי

פעילות בונוס: חשבו מהר

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

1. מכשירים שאפשר לפרוץ אליהם
2. ביטויים שנוכלים משתמשים בהם לעיתים קרובות
3. אמצעי תשלום שנוכלים מבקשים
4. סוגי הונאות באינטרנט
5. הצעות שטובות מכדי להיות אמיתיות
6. מקומות לדווח בהם על הונאה
7. מילים הקשורות לאבטחת סייבר
8. אנשים שאפשר להזהיר מפני הונאות
9. דברים שמגבים
10. סימני אזהרה באימייל
11. סימנים לכך שמחשב נדבק
12. דרכים לבדוק חנות מקוונת
13. דרכים להגן על החשבונות שלכם
14. דברים שעושים אם נפלתם להונאה
15. דברים שעושים אחרי דליפת נתונים

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

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

מקרה בוחן 1: מניעת הונאת העברה בנקאית בארגון

👨‍💻

תרחיש: מחלקת הכספים מקבלת אימייל דחוף מכתובת ספק מזויפת, המבקש להפנות העברות בנקאיות עתידיות עבור חשבוניות למספר ניתוב חדש.

שאלה לדיון: תארו בקצרה את מדיניות אימות הונאות העברה בנקאית, וציינו חסמי אימות אימייל.

מקרה בוחן 2: אירוע פישינג מסוג ציד לווייתנים נגד מנהל בכיר

👨‍💻

תרחיש: מנהל בכיר לחץ על קישור פישינג שטען להכיל מסמך מאובטח לישיבת דירקטוריון, והזין את פרטי הגישה הארגוניים הראשיים שלו בפורטל מזויף.

שאלה לדיון: פרטו את צעדי התגובה לאירוע, והסבירו כיצד לבקר את התחברויות המנהל הבכיר.

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

3	14	10	21	10	17		22	6	14	6	10	15	10	14		6	5	7
22	6	13	10	1	6		19	20	6	15		22	6	16	18	13	1	2

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 הונאה מקוונת?

תרמית שמשתמשת בערוצים דיגיטליים כדי להונות קורבנות לשלוח כסף או למסור אישורי גישה אישיים.

Q2: מהו האינדיקטור העיקרי לפישינג בדוא"ל?

הודעה שטוענת לדחיפות (כמו השעיית חשבון) ומפנה אותך לקישור שאינו תואם לדומיין הרשמי.

Q3: מהו typosquatting?

רישום דומיינים עם שגיאות הקלדה נפוצות של מותגים פופולריים (כמו amaz0n.com) כדי לארח אתרי פישינג מזויפים.

Q4: מהי הונאת תמיכה?

חלון קופץ שטוען שהמחשב שלך נגוע, ומפנה אותך להתקשר למספר ולשלם עבור תוכנת ניקוי מזויפת או שירותי גישה מרחוק. [1]

Q5: מהו vishing?

התקפות פישינג באמצעות שיחות טלפון קוליות כדי להערים על קורבנות ולגרום להם למסור פרטי חשבון בנק או פרטי כניסה.

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מה משמעות הונאת תקשורת (wire fraud)?

הפניית עסקאות תשלום לחשבונות הונאה באמצעות התחזות לספקים או למנהלים.

Q7: מהו whaling?

צורה ממוקדת מאוד של פישינג מכוון שמכוונת ישירות ליעדים בעלי ערך גבוה, כמו מנהלים בכירים בתאגידים.

Q8: מהו smishing?

הודעות טקסט הונאה שנשלחות למכשירים ניידים, ובהן קישורים לפורטלים מזויפים או לעדכוני מעקב.

Q9: מדוע אימות מחוץ לערוץ (out-of-band) קריטי?

הוא מאשר פרטי עסקה בערוץ תקשורת נפרד (כמו שיחת טלפון) ומונע שימוש בשרשורי דוא״ל שנפרצו.

Q10: כיצד פועלת הונאת חשבון נאמנות מזויף?

נוכלים יוצרים אתר חשבון נאמנות מזויף, טוענים שהכספים מוחזקים בבטחה ואז גונבים את ההעברה הבנקאית של הקונה.

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

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

Q1: כיצד נוכלים משתמשים ב-BEC (פריצה לדוא"ל עסקי) לביצוע הונאות העברה בנקאית?

הם משתלטים על חשבון הדוא"ל של עובד לגיטימי, עוקבים אחר שרשורי חשבוניות ושולחים פרטי חיוב מעודכנים עם חשבונות בנק של הונאה.

Q2: מהו הסיכון של התקפות הומוגרף IDN בהונאות מקוונות?

שימוש בתווים שאינם ASCII הנראים זהים לאותיות רגילות (למשל 'a' קירילית) כדי לרשום דומיינים מזויפים המחקים מותגים אמיתיים.

Q3: מדוע בדיקת כותרות אימייל חשובה בזיהוי הונאות?

הוא חושף את כתובת ה-IP האמיתית של שרת המקור ואת מצב אימות SPF/DKIM, ומראה אם דומיין השולח מזויף.

Q4: כיצד נוכלי תמיכה מנצלים תוכנות שולחן עבודה מרוחק?

הם משתמשים בכלים כמו AnyDesk או TeamViewer כדי להתחבר למכשיר הקורבן, להטמין נוזקה ולגנוב סיסמאות שמורות.

Q5: מהי מטרת הונאות מקדמה (advance-fee)?

הטעיית קורבנות לשלם מראש דמי טיפול בתמורה לפרס כספי גדול שאינו קיים.

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

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

Q6: כיצד נוכלים משתמשים בפרופיילינג ברשתות חברתיות לפישינג ממוקד?

הם מרכזים מבני ארגון ושמות עובדים כדי לנסח הודעות דוא"ל משכנעות של פישינג ממוקד.

Q7: מדוע חנויות אינטרנט מזויפות מציעות הנחות חדות?

כדי לפתות קונים להזין את פרטי כרטיס האשראי שלהם ולתפוס פרטי כניסה לשימוש חוזר או למכירה בפורומים של גנבי כרטיסים.

Q8: כיצד רשומות DMARC חוסמות הונאות פישינג?

DMARC מאפשר לבעלי דומיינים לבקש מהשרתים המקבלים להעביר להסגר או לדחות דואר שנכשל בבדיקות SPF ו-DKIM מותאמות, וכך לחסום זיוף ישיר. [5]

Q9: מהו האיום של פורטלים לקצירת אישורי גישה?

דפי נחיתה מתחזים שנועדו להיראות בדיוק כמו Microsoft 365 או סביבות העבודה של Google, וגונבים פרטי כניסה בזמן שהם מוקלדים.

Q10: כיצד צוותי אבטחה מדווחים על דומיינים של הונאות ומשביתים אותם?

על ידי הגשת ראיות להונאה לדוא"ל ההתעללות של הרשם, לספק האירוח ולמאגר Google Safe Browsing.

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

פישינג וזיוף היו סוג הפשע שדווח הכי הרבה ל-IC3 של ה-FBI ב-2025, עם 191,561 תלונות. [2]

2. תובנות על אבטחה

Business Email Compromise (BEC) גרם להפסדים של מעל $3 מיליארד שדווחו ל-IC3 של ה-FBI בשנת 2025. [2]

3. תובנות על אבטחה

דומיינים עם שגיאות כתיב מכוונות (typo-squatting) נבדלים משמות מותג אמיתיים בתו אחד או שניים, ולכן מבט חטוף עלול לפספס אותם.

4. תובנות על אבטחה

הונאות תמיכה טכנית גרמו להפסדים של מעל 2.1 מיליארד דולר שדווחו ל-IC3 של ה-FBI ב-2025. [2]

5. תובנות על אבטחה

התקפות הומוגרף נראות זהות בשורות הכתובת של הדפדפן, אלא אם הדפדפן מציג תצורות punycode.

6. תובנות על אבטחה

הונאות הודעות SMS (smishing) משתמשות בהודעות קצרות ודחופות עם קישורים, ומותירות לקורבנות מעט הקשר לזיהוי ההונאה.

7. תובנה על אבטחה

התקפות ווישינג מכוונות לאימיילים של בכירים משום שהם שולטים בגישה להעברות בנקאיות גדולות.

8. תובנה על אבטחה

אימות שינויי תשלום באמצעות התקשרות למספר טלפון מוכר ושמור הוא הגנה מרכזית מפני הונאת העברות BEC.

9. תובנה על אבטחה

אתרי חשבון נאמנות מזויפים הם הונאה נפוצה בשווקים מקוונים: הם נראים כשירות תשלום בטוח אך גונבים את ההעברה הבנקאית של הקונה.

10. תובנות על אבטחה

Google Safe Browsing מזהיר משתמשים לפני שהם פותחים אתרים שסומנו כאתרי פישינג או נוזקות.

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.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] 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

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

מהו האינדיקטור העיקרי להונאת תמיכה? → חלון קופץ שטוען שהמערכת שלך נגועה ודורש ממך להתקשר למספר טלפון

2 שאלה 2 — תשובה נכונה: A

הערה למורה

איזו טכניקה משתמשת בדומייני שולח מזויפים כדי לגנוב פרטי בנק? → פישינג באימייל

3 שאלה 3 — תשובה נכונה: A

הערה למורה

מה מייצג הונאת העברה בנקאית? → הונאת קורבנות כדי שישלחו כסף לחשבונות ארגוניים מזויפים באמצעות הנדסה חברתית

4 שאלה 4 — תשובה נכונה: A

הערה למורה

מדוע נוכלים יוצרים אתרי קניות מזויפים? → כדי לגנוב פרטי כרטיס אשראי ופרטי תשלום מקונים

5 שאלה 5 — תשובה נכונה: A

הערה למורה

מה משמעות וישינג? → הונאות פישינג קולי ברשתות טלפון כדי לגנוב אישורי גישה

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 **שאלה 6**

תשובה נכונה: לא נכון

הערה למורה

לא נכון: פישינג מכוון גם למנהלים בכירים; whaling הוא פישינג המכוון למנהיגים בכירים.

7 **שאלה 7**

תשובה נכונה: נכון

הערה למורה

דומיינים מתחזים משתמשים לעיתים קרובות בשגיאות הקלדה קלות (כמו amaz0n.com) כדי לחקות מותגים מהימנים.

8 **שאלה 8**

תשובה נכונה: לא נכון

הערה למורה

לא נכון: מתן גישה מרחוק לנוכל תמיכה מאפשר לו לשתול נוזקות ולגנוב נתונים.

9 **שאלה 9**

תשובה נכונה: נכון

הערה למורה

הנדסה חברתית מנצלת פסיכולוגיה אנושית כמו פחד ודחיפות כדי לעקוף כללי אבטחה.

10 **שאלה 10**

תשובה נכונה: נכון

הערה למורה

יש לאמת בקשות להעברה בנקאית תמיד באמצעות ערוצי תקשורת נפרדים (out-of-band).

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

G 1. פישינג	F 2. מזויף	D 3. וישינג	B 4. הונאה
H 5. אימות	A 6. העברה בנקאית	E 7. וויילינג	C 8. פישינג ב-SMS

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 פישינג	2 מזויפות	3 וישינג	4 הונאה
5 אימות	6 הסטה		

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

1 B – מזויפות	2 E – אימות	3 F – הסטה	4 H – סמישינג
5 G – לווייתנים	6 C – וישינג	7 A – פישינג	8 D – הונאה

הערות לדיון עבור מורים

מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את פישינג, מזויף ו-וישינג ונותנים דוגמה לכל אחד מהם.

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

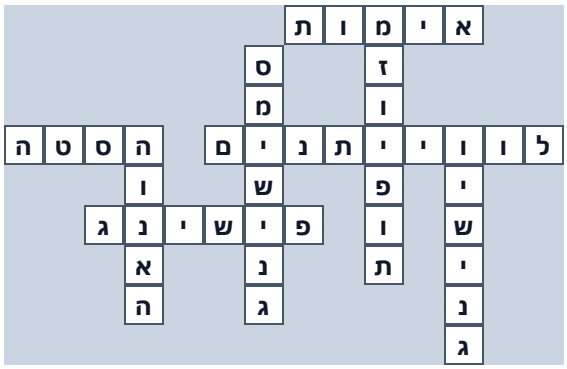
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת

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

פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

1 מאוזן: אימות אישור פרטי תשלום באמצעות שיטת קשר משנית מהימנה (5 אותיות)

4 מאוזן: לווייתנים התקפות פישינג ממוקדות שנועדו לגנוב אישורי כניסה ממנהלים בכירים (9 אותיות)

6 מאוזן: הסטה הפניה במרמה של עסקאות בנקאיות לחשבונות פושעים (4 אותיות)

7 מאוזן: פישינג קמפיינים הונאתיים בדוא"ל שנועדו לגנוב אישורי כניסה וסיסמאות (6 אותיות)

מאונך

2 מאונך: מזויפות כתובת שולח דוא"ל או אתר המדומים להיראות לגיטימיים (7 אותיות)

3 מאונך: סמישינג שליחת הודעות טקסט הונאתיות לגניבת אישורי חשבון נייד (7 אותיות)

5 מאונך: וישינג שיחות קוליות הונאתיות שנועדו לגנוב אישורי כניסה ופרטי חשבון (6 אותיות)

6 מאונך: הונאה תכסיס מרמה שנועד לגנוב כסף או גישה לאישורים מקורבנות (5 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. שפינגי — **פישינג**
2. גושניי — **וישינג**
3. מאתוי — **אימות**
4. ימייתלוו — **לווייתנים**
5. פתיומוז — **מזויפות**
6. אהנהו — **הונאה**
7. טההס — **הסטה**
8. משגסניי — **סמישינג**

מפתח אתגר הצופן הסודי

"זהו ניסיונות פישינג באמצעות סורק ואימות"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: מניעת הונאת העברה בנקאית בארגון

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מחלקת הכספים מקבלת דוא״ל דחוף מכתובת ספק מזויפת, שמבקש שהעברות עתידיות לתשלום חשבוניות יופנו למספר ניתוב חדש.
- אסטרטגיה ופתרון מומלצים: אכפו מדיניות אישור כפול לכל התשלומים. יישמו אימות חוץ-ערוצי באמצעות מספר טלפון שנשמר מראש, וחסמו בשער הדוא״ל הודעות מדומיינים מתחזים.

B מקרה בוחן 2: אירוע פישינג מסוג ציד לווייתנים נגד מנהל בכיר

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מנהל בכיר לחץ על קישור פישינג שטען שהוא מכיל מסמך מאובטח לישיבת דירקטוריון, והזין את פרטי הגישה הראשיים שלו בארגון בפורטל מזויף.
- אסטרטגיה ופתרון מומלצים: בודדו את מכשיר המנהל. אפסו את כל אסימוני ההפעלה ופרטי ההתחברות של החברה. בדקו את יומני הגישה לאיתור הוצאת נתונים, ויישמו MFA חומרתי בכל ההתחברויות.