שם: _____ תאריך: _____ ציון: _____

התקפות פישינג והנדסה חברתית

פישינג ממוקד, הונאות לוויתן (whaling), פרוטוקולי SPF/DKIM/DMARC, זיוף שולח והדרכת אבטחה לעובדים.

סקירת למידה: התקפות פישינג

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך התקפות פישינג והנדסה חברתית. תחקרו פישינג ממוקד (spear phishing), whaling, התחזות לדומיין, פרוטוקולי SPF/DKIM/DMARC, בטיחות קישורים והדרכות מודעות לעובדים.

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/phishing-attacks/

מפת הלמידה שלכם: צמצום פישינג

- זהו תרמיות נפוצות של פישינג, וישינג וחלונות קופצים של תמיכה.
- יישמו נהלי אימות עסקאות בערוץ נפרד.
- הגדירו כללי SPF, DKIM ו-DMARC כדי לחסום דומיינים מזויפים.

הוראות למדריך התקפות פישינג

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 אימות דוא"ל. ולסיום, פעילות הבונוס "חשבו מהר".

התקפות פישינג והנדסה חברתית (מבוא)

התקפות פישינג משתמשות בהודעות ממוקדות, בהונאות ציד לווייתנים ובזיוף דומיינים כדי לקצור פרטי כניסה של משתמשים. אבטחת מערכות ארגוניות מחייבת פריסה של כללי SPF, DKIM ו-DMARC בשער הכניסה לצד שלבי אישור בערוץ נפרד.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהו פישינג ממוקד (spear phishing)?
   - A. אימייל פישינג ממוקד שמותאם לאדם או לארגון ספציפיים
   - B. דוא"ל המוני רחב שנשלח למיליוני כתובות אקראיות
   - C. מתקפת רשת המציפה שרתי אינטרנט בתעבורה
   - D. טכניקת חילוץ ממסד נתונים המכוונת לרשומות משתמשים

2. איזה פרוטוקול מאפשר לדומיין לפרט ב-DNS את כתובות ה-IP המורשות לשלוח ממנו, כדי להילחם בהתחזות?
   - A. SPF
   - B. DKIM
   - C. DMARC
   - D. HTTPS

3. מהי התקפת ווילינג?
   - A. קמפיין פישינג שמכוון במיוחד למנהלים בכירים בעלי פרופיל גבוה בתאגידים
   - B. מתקפת הזרקת SQL המכוונת לגיבויי מסדי נתונים
   - C. גניבה פיזית של ציוד נתבים ברשת מקומית
   - D. סריקת כוח גס אוטומטית של Credential Stuffing

4. מה עושה DKIM?
   - A. מוסיף חתימה קריפטוגרפית לאימיילים כדי לאמת את אמינות השולח
   - B. חוסם תעבורת חבילות רשת נכנסת בחומת האש
   - C. מצפין נפחי אחסון של מסד נתונים במנוחה
   - D. סורק קבצים מצורפים בדוא"ל בחיפוש נוזקות מבוססות חתימה

5. מהו תפקידו של DMARC?
   - A. הנחיית שרתי אימייל מקבלים כיצד לטפל בבדיקות SPF/DKIM שנכשלו
   - B. פענוח סיסמאות מערכת באמצעות טבלאות קשת (rainbow tables) מחושבות מראש
   - C. דחיסת קבצים מצורפים בדוא"ל לפני המשלוח
   - D. הגדרת הרשאות גישה לניתוב רשת

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. פישינג ממוקד (spear phishing) מסתמך על דוא״ל המוני כללי הנשלח למיליוני כתובות אקראיות.

נכון לא נכון

שאלה 7

7. מדיניות DMARC יכולות להורות לשרתי דואר לדחות הודעות מזויפות שאינן מורשות.

נכון לא נכון

שאלה 8

8. אימות SPF פועל על ידי אימות החתימה הקריפטוגרפית של גוף הדוא״ל.

נכון לא נכון

שאלה 9

9. התקפות וויילינג מכוונות למנהלי מערכת זוטרים בחברות כדי לגשת לקובצי מסדי נתונים.

נכון לא נכון

שאלה 10

10. אימות מחוץ לערוץ (out-of-band) של בקשות תשלום עוזר לעצור הונאות העברה בנקאית.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. מיקוד של עובד ספציפי במידע מותאם אישית הוא פישינג _____ .
2. זיוף כותרת דוא"ל כדי שהודעות ייראו לגיטימיות הוא _____ של שולח.
3. רשימת רשומות ה-DNS של כתובות IP של שרתי דואר מורשים היא _____ .
4. תקן החתימה בדואר שמספק אימות שולח הוא _____ .
5. קביעת מדיניות לדחיית בדיקות SPF/DKIM שנכשלו נעשית באמצעות _____ .
6. קמפיין פישינג המכוון למנהלים בכירים נקרא _____ .

בנק מילים

התחזות | וישינג | ממוקד | פישינג | ציד לווייתנים | DKIM | DMARC | SPF

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

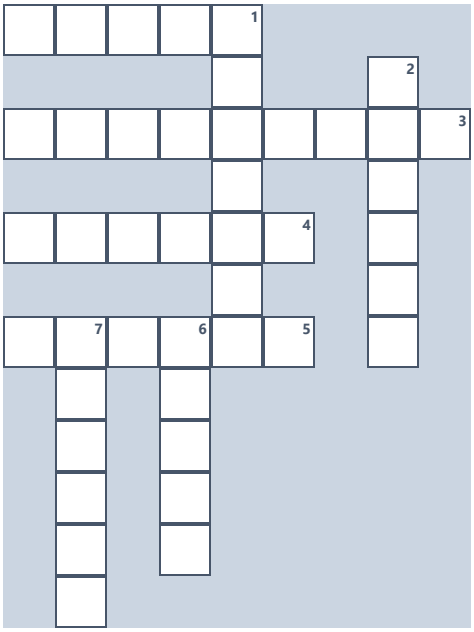
התאמת הגדרות

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

1. ממוקד		A	שיחות הונאה קוליות.
2. זיוף		B	מיקוד במנהלים בכירים בדרג C-level.
3. SPF		C	הוראות דחייה לפי מדיניות.
4. DKIM		D	כתובות IP מורשות לשליחה ב-DNS.
5. DMARC		E	דוא"ל של הנדסה חברתית.
6. ווייל‌ינג		F	הודעת דוא"ל ממוקדת ומותאמת אישית.
7. פישינג		G	זיוף כתובת הדוא"ל של השולח.
8. וישינג		H	חתימה קריפטוגרפית בדוא"ל.

נקודת ביקורת 5: תשבץ

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



מאוזן

1. הודעת דוא"ל מותאמת אישית המכוונת למטרה מסוימת (5)
3. מכוונים למנהלים בכירים (9)
4. הנדסה חברתית בהודעת דואר (6)
5. זיוף כתובת הדוא"ל של השולח (6)

מאונך

1. הוראות לדחיית הודעות (7)
2. כתובות IP המורשות ב-DNS לשליחת דואר (6)
6. מנגנון קריפטוגרפי המוטמע בהודעות דואר (5)
7. שיחות הונאה קוליות (6)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

1 מאוזן: הודעת דוא"ל מותאמת אישית המכוונת למטרה מסוימת (5 אותיות):

3 מאוזן: מכוונים למנהלים בכירים (9 אותיות):

4 מאוזן: הנדסה חברתית בהודעת דואר (6 אותיות):

5 מאוזן: זיוף כתובת הדוא"ל של השולח (6 אותיות):

מאונך

1 מאונך: הוראות לדחיית הודעות (7 אותיות):

2 מאונך: כתובות IP המורשות ב-DNS לשליחת דואר (6 אותיות):

6 מאונך: מנגנון קריפטוגרפי המוטמע בהודעות דואר (5 אותיות):

7 מאונך: שיחות הונאה קוליות (6 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

ממוקד | התחזות | שולחים | חתימה | מדיניות | לווייתנים | פישינג | וישינג

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	הגדרות ושדות התאמה
A. ממוקד	1. זיוף כתובת הדוא״ל של השולח.
B. התחזות	2. הודעת דוא״ל מותאמת אישית המכוונת למטרה מסוימת.
C. שולחים	3. שיחות הונאה קוליות.
D. חתימה	4. כתובות IP המורשות ב-DNS לשליחת דואר.
E. מדיניות	5. הנדסה חברתית בהודעת דואר.
F. לווייתנים	6. הוראות לדחיית הודעות.
G. פישינג	7. מנגנון קריפטוגרפי המוטמע בהודעות דואר.
H. וישינג	8. מכוונים למנהלים בכירים.

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. ק ו מ ד מ
2. מ ש ל י ח ו
3. נ מ י ת י ו ד
4. ג י ש נ פ י
5. ז ח ת ה ו ת
6. מ ח י ה ת
7. ת ל י ס נ י ו י ו
8. ש ג ו נ י י

פעילות בונוס: חשבו מהר

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

1	מכשירים שאפשר לפרוץ אליהם		
2	סימנים לאימייל פישינג		
3	סימנים לכך שמחשב נדבק		
4	מילים שיוצרות דחיפות מזויפת		
5	דרכים לבדוק שולח		
6	אנשים שאפשר לבקש מהם עזרה ב-IT		
7	דברים שמגבים		
8	דגים או יצורי ים שאתם מכירים		
9	חברות שנוכלים מתחזים אליהן		
10	הרגלים בטוחים שאפשר להתחיל כבר היום		
11	דברים שעושים אחרי לחיצה על קישור מזויף		
12	דברים שעושים אחרי דליפת נתונים		
13	ערוצים שבהם מתרחש פישינג		
14	דברים שלעולם לא שולחים באימייל		
15	דרכים להגן על החשבונות שלכם		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

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

מקרה בוחן 1: טיפול בהתקפת ציד לווייתנים על ההנהלה הבכירה



תרחיש: סמנכ"ל כספים מקבל אימייל מותאם אישית ביותר שטוען שהוא מהמנכ"ל, ומבקש העברה בנקאית מהירה של 50,000 דולר כדי לסגור רכישה חשאית של דומיין.

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

מקרה בוחן 2: הטמעת מדיניות שער SPF/DKIM/DMARC



תרחיש: ארגון נכשל בביקורות אבטחה משום שאימיילים שיווקיים יוצאים מסומנים לעיתים קרובות כספאם, והאקרים מתחזים באופן פעיל לדומיין המותג של החברה.

שאלה לדיון: קבעו בקרות טכניות וניהוליות לאימות אותנטיות של אימייל.

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	10	22	20	2	8		5	15	4	14	5		6	5	7
12	**10**	**10**	**13**	**10**	**1**		**20**	**16**	**21**		**22**	**20**	**6**	**19**	**10**	**2**	**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: מהו פישינג?

פישינג הוא התקפת הנדסה חברתית שבה פושעים שולחים הודעות מזויפות כדי להערים על משתמשים ולגרום להם לשתף מידע רגיש.

Q2: מה ההבדל בין פישינג לפישינג ממוקד (spear phishing)?

פישינג מכוון לקבוצות רחבות עם תוכן גנרי, ואילו פישינג ממוקד מכוון לקורבנות מסוימים באמצעות פרטים מותאמים.

Q3: מהו whaling?

וויילינג הוא התקפת פישינג ממוקדת מאוד נגד בכירים בולטים שמחזיקים בסמכות ניהולית.

Q4: מהו זיוף אימייל (email spoofing)?

זיוף דוא"ל הוא יצירת הודעות דוא"ל עם כתובת שולח מזויפת כדי להערים על הנמען לתת אמון במקור.

Q5: כיצד SPF מונע זיוף?

הוא מפרסם ב-DNS רשימה של כתובות IP מורשות לשליחה, ומאפשר לשרתים מקבלים לאמת את מקור הדואר. [1]

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מהו DKIM?

DomainKeys Identified Mail מוסיף חתימה קריפטוגרפית לכותרות דוא״ל, ומוכיח שדומיין לקח אחריות וששההודעה לא שונתה.

Q7: מה פירוש DMARC?

Domain-based Message Authentication, Reporting, and Conformance. [2]

Q8: מהי מדיניות DMARC?

מדיניות שמורה לשרתי אימייל כיצד לטפל בהודעות שנכשלות ב-SPF/DKIM (none, quarantine או reject). [2]

Q9: מהו vishing?

פישינג קולי, שבו תוקפים משתמשים בשיחות טלפון מתחזות כדי להוציא מידע ניהולי או פיננסי.

Q10: כיצד סורקי קישורים עוזרים?

הם סורקים וכותבים מחדש קישורים בדוא״ל נכנס כדי לאמת את בטיחות דפי היעד בזמן הלחיצה.

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

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

Q1: כיצד פועלת התקפת הומוגרף?

תוקפים רושמים שמות דומיין באמצעות תווי Unicode שאינם ASCII ודומים למראה, כדי לחקות באופן חזותי שם דומיין לגיטימי.

Q2: מהו ייצוג Punycode?

קידוד שממיר שמות דומיין ב-Unicode למחרוזות תואמות ASCII שמתחילות ב-'xn--' כדי ש-DNS יוכל לטפל בהם.

Q3: מדוע 'p=reject' הוא מצב DMARC הבטוח ביותר?

הוא מבקש משרתים מקבלים לדחות דואר שנכשל ב-DMARC (SPF/DKIM מיושרים) במהלך מפגש ה-SMTP, וחוסם התחזות ישירה. [2]

Q4: כיצד תוקפים עוקפים כללי SPF?

על ידי ניצול דומיינים דומים למראה (typosquatting) או שימוש בחשבונות שנפרצו בשירותי דואר לגיטימיים של צד שלישי.

Q5: מהי חדירה לאימייל עסקי (BEC)?

הונאה ארגונית שבה תוקפים חוטפים או מתחזים לחשבונות אימייל עסקיים כדי לאשר תשלומי הונאה.

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

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

Q6: כיצד אימות רב-שלבי עוצר פישינג?

הוא דורש אסימונים משניים (כמו מפתחות חומרה) שלא ניתן לגנוב באמצעות דפי נחיתה מתחזים בלבד.

Q7: מהו דף נחיתה לקצירת אישורי גישה?

פורטל התחברות מתחזה שנועד ללכוד בזמן אמת שמות משתמש, סיסמאות ואסימוני MFA שהוזנו.

Q8: מהי חטיפת תת-דומיין?

תוקף שתופס שליטה במצביע תת-דומיין DNS שאינו בשימוש כדי לארח דפי נחיתה זדוניים של פישינג תחת דומיין אב מהימן.

Q9: כיצד פועלת בדיקת יישור DKIM?

הוא מוודא שהדומיין בכותרת 'From' תואם לדומיין שחתם קריפטוגרפית על ההודעה בכותרת DKIM.

Q10: מהו תפקידה של שער דוא״ל?

סינון דוא״ל נכנס, ביקורת קישורים, הרצת קבצים מצורפים בארגז חול ואימות עמידה ב-SPF/DKIM/DMARC.

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. [4]

2. תובנות על אבטחה

פריצה לדוא״ל עסקי (BEC) גרמה להפסדים של מעל $3 מיליארד שדווחו ל-IC3 של ה-FBI בשנת 2025. [4]

3. תובנות על אבטחה

התקפות הומוגרף משתמשות באותיות קיריליות דומות כדי לשכפל חזותית דומיינים של מותגים בהתאמה מדויקת בדפדפנים.

4. תובנות על אבטחה

עם "p=reject", דומיין מבקש מהמקבלים לסרב לדואר שנכשל במהלך המסירה, ולא לסווג אותו כספאם. [2]

5. תובנות על אבטחה

התקפות וויילינג המכוונות למנכ״לים מבקשות בדרך כלל תשלומים דחופים עבור מיזוגים חסויים או רכישות דומיינים.

6. תובנות על אבטחה

פורטלים לקצירת אישורי גישה מעתיקים דפי כניסה אמיתיים כך שהקורבנות מקלידים סיסמאות ישירות בטופס של התוקף.

7. תובנה על אבטחה

ההנחיות המשותפות של CISA בנושא פישינג ממליצות על הדרכת משתמשים לצד DMARC, SPF, DKIM ו-MFA עמיד בפני פישינג. [3]

8. תובנה על אבטחה

הערכת SPF מוגבלת ל-10 מונחים שמבצעים שאילתות DNS; חריגה מהמגבלה מחזירה תוצאת 'permerror'. [1]

9. תובנה על אבטחה

מפתחות אבטחה חומרתיים FIDO2 מספקים הגנה מגובה קריפטוגרפית מפני קצירת פרטי גישה מרחוק.

10. תובנות על אבטחה

פישינג הוא אחת הדרכים הנפוצות ביותר שבהן תוקפים חודרים לראשונה לארגון, ולכן הדרכות מודעות סדירות הן הגנה יעילה.

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] IETF. (2014). RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1.

https://www.rfc-editor.org/rfc/rfc7208.html

[2] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

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

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

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

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

מפתח תשובות: נקודת ביקורת 1 – שאלות אמריקאיות

1 שאלה 1 — **תשובה נכונה: A**

הערה למורה

מהו פישינג ממוקד (spear phishing)? → אימייל פישינג ממוקד שמותאם לאדם או לארגון ספציפיים

2 שאלה 2 — **תשובה נכונה: A**

הערה למורה

SPF מפרסם ב-DNS את המארחים המורשים לשלוח עבור דומיין כדי שמקבלים יוכלו לבדוק את שולח המעטפה.

3 שאלה 3 — **תשובה נכונה: A**

הערה למורה

מהי התקפת וויילינג? → קמפיין פישינג שמכוון במיוחד למנהלים בכירים בעלי פרופיל גבוה בתאגידים

4 שאלה 4 — **תשובה נכונה: A**

הערה למורה

מה עושה DKIM? → מוסיף חתימה קריפטוגרפית לאימיילים כדי לאמת את אמינות השולח

5 שאלה 5 — **תשובה נכונה: A**

הערה למורה

מהו תפקידו של DMARC? → הנחיית שרתי אימייל מקבלים כיצד לטפל בבדיקות SPF/DKIM שנכשלו

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: לא נכון

הערה למורה

לא נכון: ספיר פישינג (spear phishing) מותאם לאנשים ספציפיים, בניגוד לפישינג המוני כללי.

7 שאלה 7

תשובה נכונה: נכון

הערה למורה

מדיניות DMARC יכולות להורות לשרתי דואר לדחות הודעות מזויפות שאינן מורשות.

8 שאלה 8

תשובה נכונה: לא נכון

הערה למורה

לא נכון: SPF בודק את כתובת ה-IP השולחת מול DNS; DKIM הוא זה שמאמת חתימה קריפטוגרפית.

9 שאלה 9

תשובה נכונה: לא נכון

הערה למורה

לא נכון: whaling מכוון למנהלים בכירים, שיכולים לאשר תשלומים ולגשת לנתונים רגישים.

10 שאלה 10

תשובה נכונה: נכון

הערה למורה

נכון: אישור בקשות תשלום דרך ערוץ נפרד ומוכר עוזר לעצור הונאות העברה בנקאית.

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

F 1. ממוקד	G 2. זיוף	D 3. SPF	H 4. DKIM
C 5. DMARC	B 6. ווילינג	E 7. פישינג	A 8. וישינג

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 ממוקד	2 התחזות	3 SPF	4 DKIM
5 DMARC	6 ציד לווייתנים		

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

1 B – התחזות	2 A – ממוקד	3 H – וישינג	4 C – שולחים
5 G – פישינג	6 E – מדיניות	7 D – חתימה	8 F – לווייתנים

הערות לדיון עבור מורים

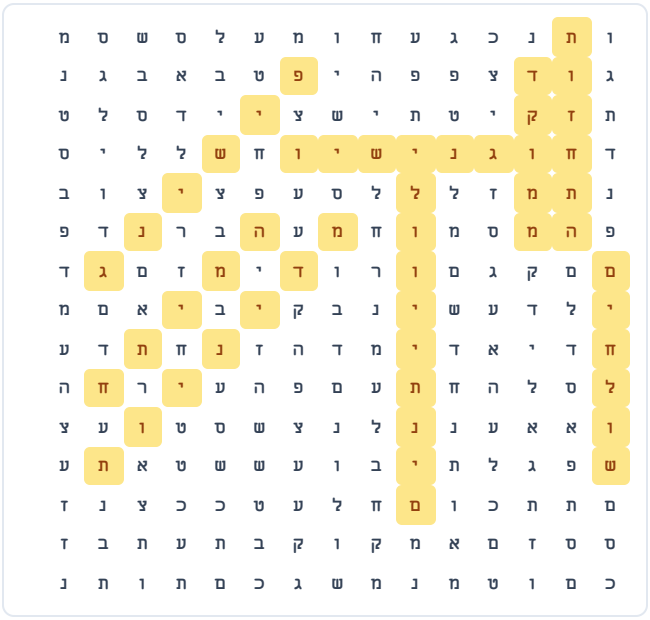
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את ממוקד, זיוף ו-SPF ונותנים דוגמה לכל אחד מהם.

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

1 מאוזן: ממוקד הודעת דוא"ל מותאמת אישית המכוונת למטרה מסוימת (5 אותיות)

3 מאוזן: לווייתנים מכוונים למנהלים בכירים (9 אותיות)

4 מאוזן: פישינג הנדסה חברתית בהודעת דואר (6 אותיות)

5 מאוזן: התחזות זיוף כתובת הדוא"ל של השולח (6 אותיות)

מאונך

1 מאונך: מדיניות הוראות לדחיית הודעות (7 אותיות)

2 מאונך: שולחים כתובות IP המורשות ב-DNS לשליחת דואר (6 אותיות)

6 מאונך: חתימה מנגנון קריפטוגרפי המוטמע בהודעות דואר (5 אותיות)

7 מאונך: וישינג שיחות הונאה קוליות (6 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. קומדמ	ממוקד	5. זחתהות	התחזות
2. משליחו	שולחים	6. מחיהת	חתימה
3. נמיתיוד	מדיניות	7. תליסניויו	לווייתנים
4. גישנפי	פישינג	8. שגוניי	וישינג

מפתח אתגר הצופן הסודי

"זהו הנדסה חברתית בביקורת שער אימייל"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: טיפול בהתקפת ציד לווייתנים על ההנהלה הבכירה

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מנהל כספים ראשי (CFO) מקבל דוא"ל מותאם אישית מאוד שמתיימר להיות מהמנכ"ל ומבקש העברה מהירה של $50,000 לסגירת רכישת דומיין חסויה.
- אסטרטגיה ופתרון מומלצים: הגדירו DMARC עם מדיניות 'p=reject' כדי לחסום דומיינים מזויפים של שולחים. הוסיפו באנרים להתרעה על שולח חיצוני בשער, ודרשו אישור בעל פה מחוץ לערוץ (out-of-band) לכל העברה כספית.

B מקרה בוחן 2: הטמעת מדיניות שער SPF/DKIM/DMARC

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: ארגון נכשל בביקורות אבטחה משום שהודעות דוא"ל שיווקיות יוצאות מסומנות לעיתים קרובות כספאם, והאקרים מתחזים באופן פעיל לדומיין המותג של החברה.
- אסטרטגיה ופתרון מומלצים: פרסמו רשומת TXT עבור SPF עם כתובות ה-IP של השולחים המורשים. הגדירו מפתחות חתימה של DKIM בשרתי הדואר היוצא, ונתחו דוחות משוב DMARC בפורמט XML שמתקבלים כדי לזהות ניצול לרעה.