שם: _____ תאריך: _____ ציון: _____

אבטחה והצפנה ב-Wi-Fi ציבורי

התקפות אדם בתווך, נקודות גישה מתחזות, האזנה לחבילות, מנהרות VPN והצפנת HTTPS.

סקירת למידה: אבטחת Wi-Fi ציבורי

ברוכים הבאים! חוברת הפעילויות הזו תדריך אתכם דרך אבטחת Wi-Fi ציבורי. תחקרו רשתות לא מוצפנות, התקפות אדם בתווך (MitM), נקודות גישה מתחזות, האזנה לחבילות, מנהרות VPN ואבטחת תעבורה ב-HTTPS.

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/public-wifi-security/

מפת הלמידה שלכם: אבטחת Wi-Fi ציבורי

- זהו סיכונים נפוצים ב-Wi-Fi ציבורי, כולל האזנה לחבילות ונקודות גישה בלתי מורשות.
- יישמו מנהרות הצפנה של VPN כדי לאבטח נתונים במעבר.
- אכפו HTTPS והגדרות דפדפן מאובטחות עבור עובדים מרחוק.

הוראות למדריך אבטחת Wi-Fi ציבורי

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 אבטחת גישה מרחוק. ולסיום, פעילות הבונוס "חשבו מהר".

אבטחת Wi-Fi ציבורי והגנה בזמן מעבר (מבוא)

נקודות Wi-Fi ציבוריות לא מוצפנות משאירות את תעבורת הרשת חשופה להאזנה למנות ולהתחזות Evil Twin. הכוונת התעבורה דרך מנהרות הצפנה מאובטחות של VPN ואכיפת כללי HSTS של HTTPS בלבד מגנות על הפעלות מפני יירוט ברשת המקומית.

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

נקודת ביקורת 1: אתגר שאלות אמריקאיות

1. מהי התקפת אדם בתווך (MitM)?

- A. יירוט ושינוי של תקשורת בין שני צדדים ברשת משותפת
- B. טכניקת חילוץ ממסד נתונים המכוונת לרשומות משתמשים
- C. הצפת שרתי אינטרנט בבקשות תעבורת רשת
- D. מחיקת כרכי האחסון בכונן הקשיח המקומי

2. מהי נקודת גישה מתחזה (Evil Twin)?

- A. נקודת Wi-Fi זדונית שהוגדרה עם אותו SSID של רשת לגיטימית
- B. כלי ניהול המשמש לניטור גיבויי מסדי נתונים
- C. תצורת שער VPN מאובטח
- D. רשומת DNS שממפה שרתי דוא"ל מורשים

3. כיצד VPN מגן על תעבורת Wi-Fi ציבורי?

- A. הוא עוטף את כל מנות הרשת במנהרה מוצפנת, כך שהן אינן קריאות למאזינים
- B. הוא חוסם אוטומטית את כל בקשות החיבור הנכנסות
- C. הוא משנה את כתובת ה-MAC של כרטיס הרשת הפיזי
- D. הוא מוחק עוגיות שמורות בדפדפן

4. מהי האזנה לחבילות (packet sniffing)?

- A. שימוש בכלי חומרה או תוכנה כדי ללכוד ולתעד מנות רשת
- B. סריקת ספריות מקומיות לאיתור קבצים כפולים
- C. הגבלת הרשאות הקריאה במסד הנתונים לפי תפקידי משתמשים
- D. הצפנת כונני אחסון באמצעות מפתחות AES-256

5. מהו תפקידו של HTTPS?

- A. הצפנת תעבורת ההפעלה בין הדפדפן לשרת האינטרנט
- B. סינון הודעות דוא"ל נכנסות בשער
- C. דחיסת תמונות לטעינת דפים מהירה יותר
- D. ניהול מבני קבצים באחסון מחובר לרשת

נקודת ביקורת 2: אתגר נכון או לא נכון

שאלה 6

6. משתמשים מחוברים יכולים ללכוד בקלות נתונים בטקסט גלוי ברשתות Wi-Fi ציבוריות פתוחות.

נכון לא נכון

שאלה 7

7. נקודות גישה סוררות (Evil Twins) תמיד מאושרות על ידי מנהלי הרשת.

נכון לא נכון

שאלה 8

8. VPN אינו יעיל בהגנה על תעבורה מפני האזנת מנות ברשתות ציבוריות.

נכון לא נכון

שאלה 9

9. HTTPS מצפין רק את נתיב ה-URL ומשאיר את תוכן החבילה בטקסט גלוי.

נכון לא נכון

שאלה 10

10. נקודות גישה Wi-Fi המשתמשות באבטחת WPA3 מציעות הגנה חזקה יותר מרשתות פתוחות וללא סיסמה.

נכון לא נכון

נקודת ביקורת 3: השלמת מונחי מפתח

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

1. לכידת סיסמאות פרטיות ברשת Wi-Fi ציבורית היא _____ של תקשורת.
2. ניתוח מנות גולמיות ברשת מקומית נעשה באמצעות _____ מנות.
3. נקודה חמה מתחזה המחקה Wi-Fi של מלון היא _____ .
4. אבטחת מעבר תעבורת אינטרנט מחייבת הצפנה באמצעות _____ .
5. הצפנת כל הפלטים של הרשת נעשית באמצעות לקוח _____ .
6. נתיב תקשורת מוצפן ברשתות ציבוריות הוא _____ .

בנק מילים

חומת אש | יירוט | מנהרה | סניפינג | תאום מרושע | HTTPS | VPN | WPA3

כתבו את תשובותיכם כאן:

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

נקודת ביקורת 4: התאמת מושגים באבטחה

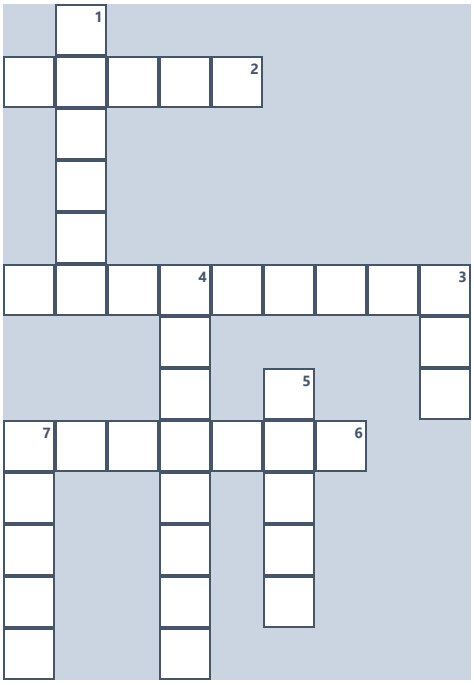
התאמת הגדרות

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

1. יירוט	A	תקן אבטחת Wi-Fi מודרני.
2. האזנה לחבילות	B	נתיב נתונים מאובטח בזמן מעבר.
3. תאום מרושע	C	סינון תעבורה נכנסת.
4. HTTPS	D	נקודת גישה סוררת שמחקה Wi-Fi.
5. VPN	E	קריאת תעבורה בזמן מעבר.
6. מנהרה	F	לכידת חבילות נתונים ברשת.
7. WPA3	G	רשת פרטית וירטואלית מוצפנת.
8. חומת אש	H	שידור מאובטח באינטרנט.

נקודת ביקורת 5: תשבץ

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



מאונן

2. קריאת תעבורה במעבר (5)

3. נקודה חמה מתחזה המחקה רשת (9) Wi-Fi

6. לכידת מנות נתוני רשת (7)

מאונך

1. סינון תעבורה נכנסת (6)

3. מפרט אבטחה מודרני ל-(3) Wi-Fi

4. רשת וירטואלית מוצפנת (8)

5. נתיב נתונים מאובטח במעבר (5)

7. העברה בטוחה של תוכן אינטרנט (5)

נקודת ביקורת 5 – פעילות חלופית: רמזים נגישים לתשבץ

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

מאוזן

2 מאוזן: קריאת תעבורה במעבר (5 אותיות):

3 מאוזן: נקודה חמה מתחזה המחקה רשת Wi-Fi (9 אותיות):

6 מאוזן: לכידת מנות נתוני רשת (7 אותיות):

מאונך

1 מאונך: סינון תעבורה נכנסת (6 אותיות):

3 מאונך: מפרט אבטחה מודרני ל-Wi-Fi (3 אותיות):

4 מאונך: רשת וירטואלית מוצפנת (8 אותיות):

5 מאונך: נתיב נתונים מאובטח במעבר (5 אותיות):

7 מאונך: העברה בטוחה של תוכן אינטרנט (5 אותיות):

נקודת ביקורת 6: חיפוש מילה נסתרת

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

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

רשימת מילים

יירוט | סניפינג | תאוממרושע | גלישה | רשתפרטית | מנהרה | תקן | חומתאש

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. יירוט	1. מפרט אבטחה מודרני ל-Wi-Fi.
B. סניפינג	2. נקודה חמה מתחזה המחקה רשת Wi-Fi.
C. תאומרושע	3. לכידת מנות נתוני רשת.
D. גלישה	4. נתיב נתונים מאובטח במעבר.
E. רשתפרטית	5. סינון תעבורה נכנסת.
F. מנהרה	6. קריאת תעבורה במעבר.
G. תקן	7. רשת וירטואלית מוצפנת.
H. חומתאש	8. העברה בטוחה של תוכן אינטרנט.

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. ו ר י ט י
2. ע ת ש ם א ר ו מ ו
3. פ ש ר ר ט ת י ת
4. ק ו ן ת
5. י ג פ י ס נ נ
6. ש ג י ה ל
7. ר ה מ ה נ
8. מ ש ח א ת ו

פעילות בונוס: חשבו מהר

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

1	סיבות לעדכן תוכנה		
2	מכשירים שמתחברים ל-Wi-Fi אוטומטית		
3	מידע שלעולם אסור לשתף		
4	הרגלים בטוחים שאפשר להתחיל כבר היום		
5	דרכים להישאר בטוחים בבית קפה		
6	מכשירים שאפשר לפרוץ אליהם		
7	דברים שהאקר יכול לראות ב-Wi-Fi פתוח		
8	סימנים לרשת Wi-Fi מזויפת		
9	חלופות ל-Wi-Fi ציבורי		
10	סימני אזהרה באימייל		
11	דברים שלא עושים ב-Wi-Fi ציבורי		
12	מקומות עם Wi-Fi חינמי		
13	דרכים להגן על החשבונות שלכם		
14	סימנים לכך שמחשב נדבק		
15	שמות Wi-Fi שנראים חשודים		

נקודת ביקורת 8: מקרי בוחן באבטחת סייבר

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

מקרה בוחן 1: בלימת האזנה לחבילות ב-Wi-Fi ציבורי



תרחיש: מנהל מכירות מרחוק המחובר לרשת Wi-Fi ציבורית בשדה תעופה מבחין שכמה אימיילים עסקיים רגישים דלפו זמן קצר לאחר ששלח אותם בטקסט גלוי.

שאלה לדיון: נתחו את סיכוני הרשת הציבורית, ותארו בקצרה פתרון להצפנת התעבורה.

מקרה בוחן 2: הגנה מפני נקודה חמה זדונית מסוג Evil Twin



תרחיש: תוקפים פורסים נקודת גישה אלחוטית מתחזה בשם "CoffeeShop_Guest" המחקה נקודת גישה לגיטימית של בית קפה, ולוכדים תעבורת רשת מאורחים שאינם חושדים.

שאלה לדיון: פרטו את שלבי האימות לזיהוי וחסימה של נקודות גישה מתחזות.

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	21	20		22	20	6	2	16	22		6	14	10	17	18	5	
5	20	5	14	13		22	20	7	16	2		22	10	20	6	2	10	18

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: מדוע Wi-Fi ציבורי אינו מאובטח?

רשת Wi-Fi ציבורית פתוחה אינה מצפינה תעבורה באוויר, ולכן אחרים בקרבת מקום יכולים ללכוד כל נתון לא מוגן. [2]

Q2: מהו ציתות לחבילות?

מאזין למנות (packet sniffer) לוכד נתונים גולמיים שזורמים בממשק רשת, וחושף סיסמאות בטקסט גלוי ופרטי תעבורה.

Q3: מהו Evil Twin?

נקודת גישה מתחזה שהוקמה על ידי האקרים ומחקה את השם וההגדרות של נקודת Wi-Fi מקומית מהימנה.

Q4: כיצד VPN מגן עלייך?

הוא מנתב את התעבורה שלכם דרך מנהרה מוצפנת ומסתיר את פעילות הגלישה שלכם מפני מאזינים ברשת המקומית.

Q5: האם HTTPS מגן עליי ב-Wi-Fi ציבורי?

כן, הוא מצפין את הנתונים המוחלפים בין הדפדפן לאתר, ו-VPN מוסיף שכבת הגנה נוספת.

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

עיינו בשאלות ותשובות נפוצות בנושא צמצום איומים ברשת.

Q6: מהו WPA3?

תקן Wi-Fi Protected Access המודרני, המציע הצפנה חזקה יותר והגנה מפני התקפות מילון לא מקוונות. [1]

Q7: האם Wi-Fi ציבורי יכול להעביר נוזקות?

כן, תוקפים יכולים ליירט תעבורה ולהזריק בקשות הורדה זדוניות (הורדות drive-by) לסשן הדפדפן שלכם.

Q8: מהו הסיכון בשיתוף קבצים?

אם שיתוף קבצים מופעל, משתמשים אחרים ברשת הציבורית יכולים לקרוא או לשנות את ספריית התיקיות המקומית שלכם.

Q9: מהו captive portal?

דף הכניסה שרשתות מלונות או בתי קפה משתמשות בו כדי להעניק גישה לאינטרנט, ושלעיתים תוקפים יכולים לזייף.

Q10: האם כדאי לכבות את ה-Wi-Fi כשלא משתמשים בו?

כן, כיבוי ה-Wi-Fi מונע מהמכשיר להתחבר אוטומטית לרשתות לא מהימנות.

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

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

Q1: כיצד התקפת אדם באמצע מנצלת DNS?

על ידי שימוש בהתחזות (DNS spoofing) DNS בנתב זדוני כדי להפנות דפדפני יעד לדפי נחיתה דומים של פישינג במקום לדומייני היעד.

Q2: מהי חטיפת הפעלה (session hijacking)?

תוקף שמאזין לעוגיית הפעלה לא מוצפנת ב-Wi-Fi ציבורי ומייבא אותה כדי לעקוף התחברות באמצעות אישורי גישה.

Q3: מהו SSL stripping?

התקפת אדם-באמצע (MitM) שבה תוקף מוריד את בקשת ה-HTTPS המאובטחת של משתמש ל-HTTP לא מוצפן ולוכד פרטי התחברות בטקסט גלוי.

Q4: כיצד HSTS מגן מפני SSL stripping?

HTTP Strict Transport Security מאלץ דפדפנים להתחבר רק דרך HTTPS ומסרב לחזרה לחיבורי HTTP לא מוצפנים. [3]

Q5: מהו VPN עם מנהור מפוצל (split-tunnel)?

הגדרת ניתוב שמעבירה רק תעבורה ארגונית דרך ה-VPN ושולחת נתוני אינטרנט ציבוריים ישירות, מה שעלול לסכן בחשיפת נתיב דליפה.

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

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

Q6: מדוע WPA2 פגיע ל-KRACK?

התקפת Key Reinstallation מנצלת את לחיצת היד בת ארבעת השלבים של WPA2 כדי לפענח מנות ללא סיסמת ה-Wi-Fi.

Q7: מהי בידוד לקוחות (client isolation)?

הגדרת אבטחה בנתב שמונעת ממכשירי Wi-Fi מחוברים לתקשר זה עם זה ישירות, וחוסמת האזנה מקומית.

Q8: כיצד תוקפים משתמשים בשרתי DNS מזויפים?

הם מגדירים נתבים זדוניים שמקצים ללקוחות שרתי DNS מזויפים, ובכך מיירטים וכותבים מחדש את כל חיפושי האינטרנט.

Q9: האם VPN יכול להסתיר את כתובת ה-MAC המקומית שלי?

לא. כתובות MAC הן מזהים מקומיים בשכבה 2; השתמשו במקום זאת בהגדרת הרנדומיזציה המובנית של כתובת MAC במכשיר שלכם (כתובת פרטית).

Q10: מהי התקפת זיוף של captive portal?

תוקף שמארח פורטל אימות מזויף בנקודה מתחזה כדי לגנוב אישורי גישה במסווה של גישה חינמית ל-Wi-Fi.

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

עובדים מרחוק משתמשים לעיתים קרובות ב-Wi-Fi בבתי קפה, במלונות ובשדות תעופה, שם אין להם שליטה באבטחת הרשת.

2. תובנות על אבטחה

נקודת גישה מתחזה מסוג Evil Twin יכולה להעתיק את השם וכתובת ה-MAC המדויקים של רשת מהימנה ולבלבל מכשירים.

3. תובנות על אבטחה

תוכנות ציתות לחבילות כמו Wireshark חינמיות ויכולות להציג סיסמאות HTTP לא מוצפנות בטקסט גלוי.

4. תובנות על אבטחה

אבטחת WPA3 משתמשת באימות סימולטני בין שווים (SAE) כדי להגן מפני התקפות כוח גס מקומיות.

5. תובנות על אבטחה

התקפות SSL stripping עוקפות הגנות HTTPS בסיסיות על ידי יירוט הפניות HTTP ראשוניות בשער.

6. תובנות על אבטחה

כותרות תגובה של HTTP Strict Transport Security (HSTS) מונעות מדפדפנים לחזור לחיבורי HTTP לא מוצפנים. [3]

7. תובנה על אבטחה

כיבוי 'Auto-Connect' מונע מסמארטפונים להתחבר לרשתות זדוניות מתחזות במרחבים ציבוריים.

8. תובנה על אבטחה

תצורות VPN ארגוניות מסוג 'always-on' מכריחות את כל תעבורת הרשת של עובדים מרחוק לעבור דרך חומות אש ארגוניות.

9. תובנה על אבטחה

נקודות גישה סוררות יכולות להחזיר תשובות DNS מזויפות ולהפנות דומיינים לשרתי פישינג.

10. תובנות על אבטחה

ללא VPN, משתמשים אחרים בנקודת גישה פתוחה יכולים לראות לאילו אתרים ושרתים המכשיר שלכם פונה.

מקורות והפניות טכניים

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

מקורות אקדמיים ותעשייתיים

[1] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

[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

מהי התקפת אדם בתווך (MitM)? → יירוט ושינוי של תקשורת בין שני צדדים ברשת משותפת

2 שאלה 2 — תשובה נכונה: A

הערה למורה

מהי נקודת גישה מתחזה (Evil Twin)? → נקודת Wi-Fi זדונית שהוגדרה עם אותו SSID של רשת לגיטימית

3 שאלה 3 — תשובה נכונה: A

הערה למורה

כיצד VPN מגן על תעבורת Wi-Fi ציבורי? → הוא עוטף את כל מנות הרשת במנהרה מוצפנת, כך שהן אינן קריאות למאזינים

4 שאלה 4 — תשובה נכונה: A

הערה למורה

מהי האזנה לחבילות (packet sniffing)? → שימוש בכלי חומרה או תוכנה כדי ללכוד ולתעד מנות רשת

5 שאלה 5 — תשובה נכונה: A

הערה למורה

מהו תפקידו של HTTPS? → הצפנת תעבורת ההפעלה בין הדפדפן לשרת האינטרנט

מפתח תשובות: נקודת ביקורת 2 – נכון או לא נכון

6 שאלה 6

תשובה נכונה: נכון

הערה למורה

משתמשים מחוברים יכולים ללכוד בקלות נתונים בטקסט גלוי ברשתות Wi-Fi ציבוריות פתוחות.

7 שאלה 7

תשובה נכונה: לא נכון

הערה למורה

לא נכון: Evil Twin הוא נקודת גישה לא מורשית שמקים תוקף כדי לחקות נקודה אמיתית.

8 שאלה 8

תשובה נכונה: לא נכון

הערה למורה

לא נכון: VPN מצפין תעבורה במנהרה, ולכן מאזינים מקומיים אינם יכולים לקרוא אותה.

9 שאלה 9

תשובה נכונה: לא נכון

הערה למורה

לא נכון: HTTPS מצפין את כל חילופי ה-HTTP, כולל נתיב ה-URL ותוכן הדף.

10 שאלה 10

תשובה נכונה: נכון

הערה למורה

נקודות גישה Wi-Fi המשתמשות באבטחת WPA3 מציעות הגנה חזקה יותר מרשתות פתוחות וללא סיסמה.

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

E 1. יירוט	F 2. האזנה לחבילות	D 3. תאום מרושע	H 4. HTTPS
G 5. VPN	B 6. מנהרה	A 7. WPA3	C 8. חומת אש

נקודת ביקורת 3: מפתח תשובות – מונחי מפתח

1 יירוט	2 סניפינג	3 תאום מרושע	4 HTTPS
5 VPN	6 מנהרה		

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

1 G – תקן	2 C – תאוממרושע	3 B – סניפינג	4 F – מנהרה
5 H – חומתאש	6 A – יירוט	7 E – רשתפרטית	8 D – גלישה

הערות לדיון עבור מורים

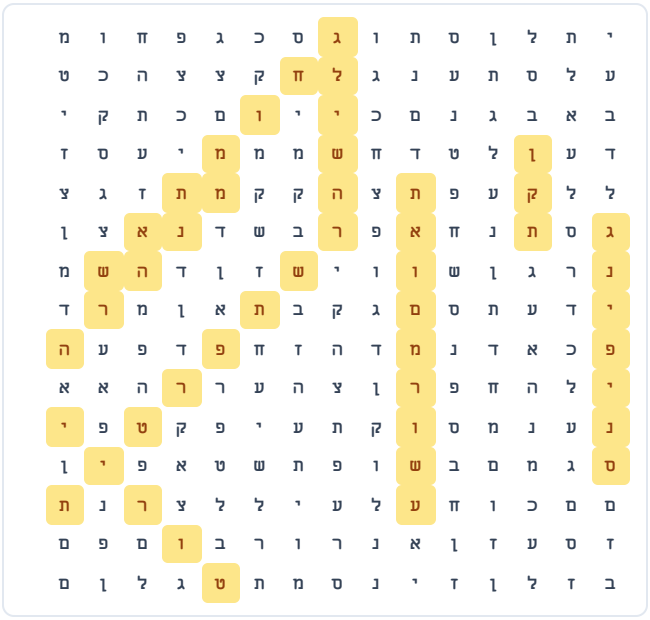
מונחי מפתח:
ודאו שהתלמידים מסבירים במילים שלהם את יירוט, האזנה לחבילות ו-תאום מרושע ונותנים דוגמה לכל אחד מהם.

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

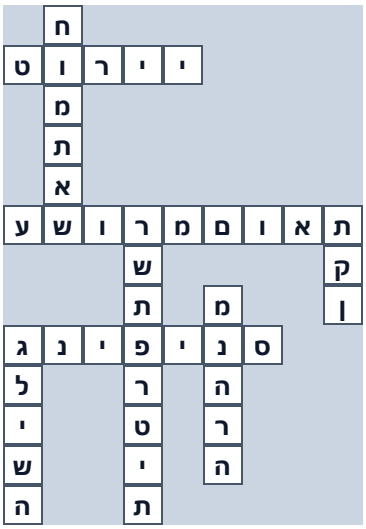
הערכת מקורות:
בקשו מהתלמידים לאמת לפחות טענה אחת במקורות של דף העבודה, ודונו מדוע נתונים, מחירים וכללים עשויים להשתנות עם הזמן.

מפתחות פאזלים והערות למורה

פתרון תפזורת



פתרון תשבץ



מדריך למורה לפתרונות התשבץ

מאוזן

2 מאוזן: יירוט קריאת תעבורה במעבר (5 אותיות)

3 מאוזן: תאוסמרושע נקודה חמה מתחזה המחקה רשת Wi-Fi (9 אותיות)

6 מאוזן: סניפינג לכידת מנות נתוני רשת (7 אותיות)

מאונך

1 מאונך: חומתאש סינון תעבורה נכנסת (6 אותיות)

3 מאונך: תקן מפרט אבטחה מודרני ל-Wi-Fi (3 אותיות)

4 מאונך: רשתפרטית רשת וירטואלית מוצפנת (8 אותיות)

5 מאונך: מנהרה נתיב נתונים מאובטח במעבר (5 אותיות)

7 מאונך: גלישה העברה בטוחה של תוכן אינטרנט (5 אותיות)

מפתח פתרונות: מילים מבולבלות ופענוח הצופן

מפתח הערכה לפעילות פענוח מילות אוצר המילים ולאתגר הצופן הסודי.

מפתח פענוח מילים מבולבלות

1. וריטי — יירוט
2. עתשמארומו — תאומרושע
3. פשררטתית — רשתפרטית
4. קות — תקן
5. יגפיסנג — סניפינג
6. שגיהל — גלישה
7. רהמהנ — מנהרה
8. משחאתו — חומתאש

מפתח אתגר הצופן הסודי

"הצפינו תעבורת רשת ציבורית בעזרת מנהרה"

מפתח תשובות למקרי הבוחן

A מקרה בוחן 1: בלימת האזנה לחבילות ב-Wi-Fi ציבורי

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: מנהל מכירות מרחוק המחובר לרשת Wi-Fi ציבורית בשדה תעופה מבחין שכמה הודעות דוא״ל עסקיות רגישות דלפו זמן קצר לאחר שנשלחו בטקסט גלוי.
- אסטרטגיה ופתרון מומלצים: חייבו שימוש בלקוח VPN ארגוני בכל תחנות העבודה מרחוק. אכפו תוספי דפדפן של HTTPS בלבד, וחסמו פרוטוקולים לא מוצפנים (כמו HTTP ו-FTP) בחומת האש של הלקוח.

B מקרה בוחן 2: הגנה מפני נקודה חמה זדונית מסוג Evil Twin

פתרון למורה

הנחיות הערכה

תשובות התלמידים צריכות לכלול את הנקודות הבאות:

- ניתוח תרחיש: תוקפים מפעילים נקודת גישה אלחוטית מתחזה בשם 'CoffeeShop_Guest' המחקה נקודת גישה לגיטימית של בית קפה, ולוכדים תעבורת רשת של אורחים תמימים.
- אסטרטגיה ופתרון מומלצים: בצעו ביקורת על כתובות MAC מסוג BSSID של נקודות גישה כדי לאמת את אותנטיות הרשת. אכפו אימות מצב לקוח כדי לחסום חיבור לרשתות פתוחות, והורו על שימוש בנקודות חמות סלולריות לעבודה רגישה.