الاسم: _____ التاريخ: _____ الدرجة: _____

أمان Wi-Fi العام والتشفير

هجمات الوسيط، ونقاط الوصول المارقة، والتقاط الحزم، وأنفاق VPN، وتشفير HTTPS.

نظرة عامة على التعلّم: أمان Wi-Fi العام

مرحبًا! ترشدك حزمة الأنشطة هذه عبر أمان شبكات Wi-Fi العامة. ستستكشف الشبكات غير المشفرة وهجمات الوسيط (MitM) ونقاط الوصول المارقة والتنصت على الحزم وأنفاق VPN وأمان النقل عبر HTTPS.

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

نقاط التحقق في ورقة العمل

- [ ] **الجزء 1-4: أتقن الأمن السيبراني ومنع التهديدات.**
- [ ] **الجزء 5-7: حل الكلمات المتقاطعة وألغاز البحث عن الكلمات.**
- [ ] **الجزء 8-9: حل دراسات الحالة وتحدي الشيفرة.**
- [ ] **الجزء 10: راجع صفحات الأسئلة الشائعة الأساسية والمتقدمة.**
- [ ] **الجزء 11: استكشف 10 حقائق مثيرة من الواقع.**
- [ ] **إضافي: تحدّي فكّر بسرعة**

افتح دليل VPN.com للأمن السيبراني

URL: https://www.vpn.com/cybersecurity/public-wifi-security/

خارطة طريقك لتعلّم أمان شبكات Wi-Fi العامة

- تعرّف على مخاطر Wi-Fi العامة الشائعة، ومنها التنصت على الحزم ونقاط الوصول المارقة.
- طبّق أنفاق تشفير VPN لتأمين البيانات أثناء النقل.
- افرض HTTPS وإعدادات المتصفح الآمنة للعاملين عن بُعد.

تعليمات دليل أمان Wi-Fi العام

أجب عن أسئلة الاختيار من متعدد وأسئلة صحيح/خطأ، وأكمل الجمل الناقصة باستخدام بنك الكلمات، وطابق التعريفات، وحُلّ الكلمات المتقاطعة وبحث الكلمات. طبّق معرفتك على أمان الوصول عن بُعد. واختم بالنشاط الإضافي «فكّر بسرعة».

أمان Wi-Fi العام وحماية العبور (مقدمة)

تترك نقاط Wi-Fi العامة غير المشفرة حركة مرور الشبكة معرّضة لالتقاط الحزم وانتحال Evil Twin. ويحمي إجبار حركة المرور على المرور عبر أنفاق تشفير VPN آمنة وفرض قواعد HSTS لـ HTTPS فقط الجلسات من الاعتراض على الشبكة المحلية.

اقرأ كل نقطة تحقق بعناية، ثم اختر الإجابة الصحيحة أو اكتبها.

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما هو هجوم الوسيط (MitM)؟

- A. اعتراض الاتصالات بين طرفين وتعديلها على شبكة مشتركة
- B. أسلوب استخراج قواعد بيانات يستهدف سجلات المستخدمين
- C. إغراق خوادم الويب بطلبات حركة الشبكة
- D. مسح وحدات تخزين القرص الصلب المحلي

2. ما هي نقطة الوصول المارقة (التوأم الشرير)؟

- A. نقطة Wi-Fi خبيثة مهيأة بالـ SSID نفسه لشبكة شرعية
- B. أداة إدارية تُستخدم لمراقبة النسخ الاحتياطية لقواعد البيانات
- C. إعداد بوابة VPN آمنة
- D. سجل DNS يربط خوادم البريد المصرح بها

3. كيف يحمي VPN حركة Wi-Fi العامة؟

- A. يغلّف جميع حزم الشبكة في نفق مشفّر، فتصبح غير مقروءة لأدوات التنصت
- B. يحظر تلقائيًا جميع طلبات الاتصال الواردة
- C. يغيّر عنوان MAC لبطاقة الشبكة الفعلية
- D. يحذف ملفات تعريف الارتباط المخزنة مؤقتًا في متصفح الويب

4. ما هو التنصت على الحزم؟

- A. استخدام أدوات عتادية أو برمجية لالتقاط حزم الشبكة وتسجيلها
- B. فحص الأدلة المحلية بحثًا عن ملفات مكررة
- C. تقييد صلاحيات قراءة قاعدة البيانات بحسب أدوار المستخدمين
- D. تشفير أقراص التخزين باستخدام مفاتيح AES-256

5. ما دور HTTPS؟

- A. تشفير حركة الجلسة بين المتصفح وخادم الويب
- B. تصفية رسائل البريد الإلكتروني الواردة عند البوابة
- C. ضغط الصور لتسريع تحميل الصفحات
- D. إدارة هياكل الملفات في التخزين المتصل بالشبكة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. يستطيع المستخدمون المتصلون التقاط البيانات النصية العادية بسهولة على شبكات Wi-Fi العامة المفتوحة.

صحيح خطأ

7 سؤال 7

7. نقاط الوصول المارقة (Evil Twins) يصرح بها مسؤولو الشبكات دائمًا.

صحيح خطأ

8 سؤال 8

8. VPN غير فعّال في حماية حركة المرور من التقاط الحزم على الشبكات العامة.

صحيح خطأ

9 سؤال 9

9. يشفّر HTTPS مسار عنوان URL فقط، ويترك حمولة الحزمة بنص عادي.

صحيح خطأ

10 سؤال 10

10. توفر نقاط Wi-Fi الساخنة التي تستخدم أمان WPA3 حماية أقوى من الشبكات المفتوحة بلا كلمة مرور.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

اقرأ كل جملة أدناه وأكمل الفراغ بالمصطلح الصحيح من بنك الكلمات.

1. التقاط كلمات المرور الخاصة على Wi-Fi العامة هو _____ للاتصالات.
2. يستخدم تحليل الحزم الخام في الشبكة المحلية أسلوب _____ على الحزم.
3. نقطة اتصال مارقة تحاكي Wi-Fi فندق هي _____ .
4. يتطلب تأمين نقل حركة الويب التشفير باستخدام _____ .
5. يستخدم تشفير جميع مخرجات الشبكة عميل _____ .
6. مسار الاتصال المشفر عبر الشبكات العامة هو _____ .

بنك كلمات المفردات

اعتراض | الآمن | التنصت | التوأم الشرير | النفق | شبكة خاصة | HTTPS | VPN

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

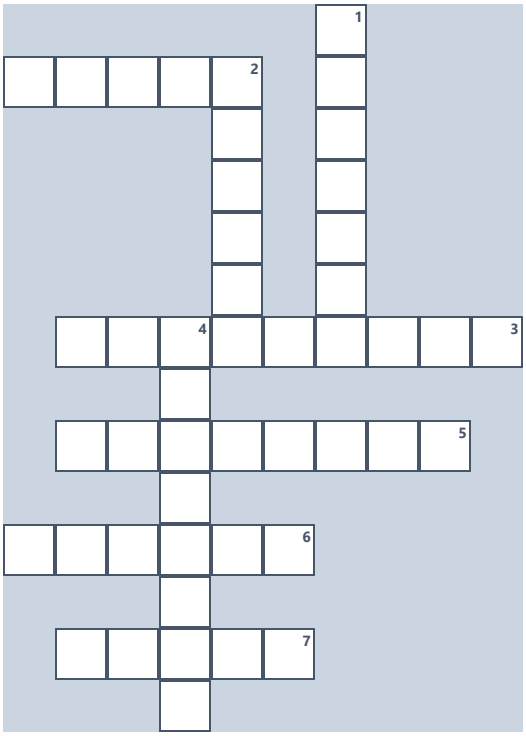
مطابقة التعريفات

طابق كل مصطلح مفردات على اليمين مع تعريفه الصحيح على اليسار بكتابة الحرف المقابل (A-H) في مربع الإدخال القابل للتعبئة.

1. الاعتراض	A	معيار أمان Wi-Fi حديث.
2. التنصت	B	مسار بيانات آمن أثناء النقل.
3. التوأم الشرير	C	تصفية حركة المرور الواردة.
4. HTTPS	D	نقطة اتصال مارقة تحاكي Wi-Fi.
5. VPN	E	قراءة الحركة أثناء النقل.
6. النفق	F	التقاط حزم بيانات الشبكة.
7. WPA3	G	شبكة افتراضية خاصة مشفّرة.
8. جدار الحماية	H	نقل آمن عبر الويب.

نقطة التحقق 5: لغز الكلمات المتقاطعة

حلّ الكلمات المتقاطعة بكتابة الحروف في المربعات البيضاء النشطة. تتوافق الأرقام مع الدلائل أدناه.



أفقي

2. مسار بيانات آمن أثناء النقل (5)

3. تصفية الحركة الواردة (9)

5. شبكة افتراضية مشفرة (8)

6. التقاط حزم بيانات الشبكة (6)

7. نقل الويب المؤمن (5)

عمودي

1. معيار حديث لأمان Wi-Fi (7)

2. نقطة اتصال مارقة تحاكي شبكة Wi-Fi (6)

4. قراءة الحركة أثناء انتقالها (8)

نقطة التحقق 5 – نشاط بديل: أدلة الكلمات المتقاطعة الميسَّرة

يمكن لمستخدمي قارئ الشاشة ولوحة المفاتيح كتابة إجابات الكلمات المتقاطعة مباشرة في حقول النص أدناه.

أفقي

2 أفقي: مسار بيانات آمن أثناء النقل (5 حروف):

3 أفقي: تصفية الحركة الواردة (9 حروف):

5 أفقي: شبكة افتراضية مشفرة (8 حروف):

6 أفقي: التقاط حزم بيانات الشبكة (6 حروف):

7 أفقي: نقل الويب المؤمن (5 حروف):

عمودي

1 عمودي: معيار حديث لأمان Wi-Fi (7 حروف):

2 عمودي: نقطة اتصال مارقة تحاكي شبكة Wi-Fi (6 حروف):

4 عمودي: قراءة الحركة أثناء انتقالها (8 حروف):

نقطة التحقق 6: البحث عن الكلمة المخفية

ابحث عن 8 مصطلحات مفردات رئيسية مخبأة في الشبكة أدناه. يمكن أن تكون الكلمات أفقية أو رأسية أو قطرية.

ت	م	م	س	د	ف	ل	ط	ك	ض	ك	ف	ت	ه	م
ن	ح	ا	ص	ش	ب	ا	ب	ت	ا	ق	ض	ص	ش	ة
ص	ض	و	ه	ص	ج	ل	ع	ش	ل	ج	س	ع	ع	ص
ك	ق	ت	ت	س	ن	ت	ل	ا	ر	م	ع	ع	ك	ل
ة	م	ل	ه	ن	ج	ر	ت	م	ك	ف	ع	ز	م	ب
ص	ي	ا	ج	ن	د	خ	ا	و	ن	ت	خ	ي	ي	د
ا	ص	ز	خ	ج	ا	ع	ج	ل	ل	م	ض	ق	ا	ت
خ	ه	ب	ا	خ	ر	ف	ج	ص	ا	ا	ا	ج	ف	ر
ة	ج	د	ر	س	ح	ج	ل	ك	ع	ع	ح	ل	س	م
ك	خ	ن	د	ل	م	ا	و	ح	ا	ا	ت	ل	ا	ق
ب	ع	ك	ه	ض	ا	ل	ك	ش	م	ه	م	ر	ت	ع
ش	ة	ب	د	م	ي	ن	ض	ي	س	ا	ل	خ	ا	ة
ة	ص	ر	س	ع	ة	ف	ل	ش	ط	ط	ن	ق	ر	ض
ك	ل	ر	خ	ا	ف	ق	و	د	و	ب	ة	م	ة	ب
ر	ط	خ	ر	ش	ف	ك	ف	ي	ت	ط	خ	ة	د	ة

قائمة كلمات المفردات

الاعتراض التنصت التوام الامن شبكةخاصة النفق المعيار جدارحماية

نقطة التحقق 6 – نشاط بديل: مطابقة المفردات الميسَّرة

طابق كل مصطلح من المصطلحات الـ 8 في البحث عن الكلمات مع تعريفه الصحيح بكتابة الحرف (A-H) في الفراغ.

مصطلحات المفردات
A. الاعتراض
B. التنصت
C. التوام
D. الامن
E. شبكةخاصة
F. النفق
G. المعيار
H. جدارحماية

التعريفات وحقول المطابقة
1. معيار حديث لأمان Wi-Fi.
2. نقطة اتصال مارقة تحاكي شبكة Wi-Fi.
3. التقاط حزم بيانات الشبكة.
4. مسار بيانات آمن أثناء النقل.
5. تصفية الحركة الواردة.
6. قراءة الحركة أثناء انتقالها.
7. شبكة افتراضية مشفرة.
8. نقل الويب المؤمن.

نقطة التحقق 7: تحدي الكلمات المبعثرة

أعد ترتيب الحروف أدناه للكشف عن المفاهيم والمصطلحات الأساسية في الأمن السيبراني. اكتب إجاباتك في مربعات الإدخال المخصصة.

1. اعتارلضا _____
2. ماتاول _____
3. ةبشخاةصك _____
4. رلييعاام _____
5. نتتاصل _____
6. ماانل _____
7. فقانل _____
8. ةحيجردماا _____

نشاط إضافي: فكّر بسرعة

اكتب 3 إجابات لكل فئة. يفوز أول من يكمل القائمة.

1. أسباب لتحديث البرامج
2. أجهزة تتصل تلقائيًا بشبكة Wi-Fi
3. معلومات لا ينبغي أن تشاركها أبدًا
4. عادات آمنة يمكنك البدء بها اليوم
5. طرق للبقاء آمنًا في مقهى
6. أجهزة يمكن اختراقها
7. أشياء يستطيع المخترق رؤيتها على شبكة Wi-Fi مفتوحة
8. علامات شبكة Wi-Fi مزيفة
9. بدائل لشبكة Wi-Fi العامة
10. علامات تحذيرية في البريد الإلكتروني
11. أشياء لا تفعلها على شبكة Wi-Fi عامة
12. أماكن فيها Wi-Fi مجاني
13. طرق لحماية حساباتك
14. علامات إصابة الحاسوب
15. أسماء شبكات Wi-Fi تبدو مشبوهة

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: احتواء التقاط الحزم على شبكة Wi-Fi العامة



السيناريو: يلاحظ مسؤول مبيعات عن بُعد متصل بشبكة Wi-Fi عامة في المطار أن عدة رسائل بريد إلكتروني تجارية حساسة تسرّبت بعد إرسالها بوقت قصير كنص عادي.

سؤال للنقاش: حلّل مخاطر الشبكات العامة، ولخّص حلًا لتشفير الحركة.

دراسة الحالة 2: الدفاع ضد نقطة الاتصال الوهمية التوأم الشريرة



السيناريو: ينشر المهاجمون نقطة وصول لاسلكية مارقة باسم 'CoffeeShop_Guest' تحاكي نقطة اتصال مقهى حقيقية، فتلتقط حركة الشبكة من الضيوف غير المنتبهين.

سؤال للنقاش: فصّل خطوات التحقق لاكتشاف نقاط الوصول المارقة وحظرها.

نقطة التحقق 9: فك الشيفرة

يحمي متخصص الأمن السيبراني أصول الشبكة من الجهات التهديدية عبر الإنترنت. استخدم مفتاح الحرف إلى الرقم أدناه لفك تشفير الرسالة بكتابة الحروف المطابقة في الفراغات.

مفتاح التشفير من الحرف إلى الرقم

ا=1 ب=2 ت=3 ث=4 ج=5 ح=6 خ=7 د=8 ذ=9 ر=10 ز=11

س=12 ش=13 ص=14 ض=15 ط=16 ظ=17 ع=18 غ=19 ف=20 ق=21 ك=22

ل=23 م=24 ن=25 هـ=26 و=27 ي=28 ة=29 ى=30 ء=31 ؤ=32 ئ=33

3	1	22	2	13	23	1		29	22	10	6		10	20	13

29	14	1	7		29	22	2	13	2		29	24	1	18	23	1

الرسالة بعد فك التشفير:

نصيحة: يمثل كل رقم حرفًا عربيًا واحدًا من المفتاح أعلاه.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء A)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q1: لماذا لا يُعد Wi-Fi العام آمنًا؟

لا تشفّر شبكات Wi-Fi العامة المفتوحة حركة المرور عبر الهواء، لذا يمكن لمن حولك التقاط أي بيانات غير محمية. [2]

Q2: ما التقاط الحزم (packet sniffing)؟

يلتقط محلل الحزم البيانات الخام المتدفقة عبر واجهة شبكة، فيكشف كلمات المرور النصية الصريحة وتفاصيل الحركة.

Q3: ما التوأم الشرير (Evil Twin)؟

نقطة وصول مارقة ينشئها المخترقون وتحاكي اسم نقطة Wi-Fi محلية موثوقة وإعداداتها.

Q4: كيف يحميني VPN؟

يوجّه حركة بياناتك عبر نفق مشفر، مخفيًا نشاط تصفحك عن متنصتي الشبكة المحلية.

Q5: هل يحميني HTTPS على شبكات Wi-Fi العامة؟

نعم، يشفّر البيانات المتبادلة بين متصفحك والموقع، ويضيف VPN طبقة حماية أخرى.

نقطة التحقق 10: الأسئلة الشائعة الأساسية حول الأمن السيبراني (الجزء B)

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ما WPA3؟

معيار الوصول المحمي بـ Wi-Fi الحديث، ويوفر تشفيرًا أقوى وحماية من هجمات القاموس دون اتصال. [1]

Q7: هل يمكن لشبكة Wi-Fi العامة نقل برمجيات خبيثة؟

نعم، يمكن للمهاجمين اعتراض الحركة وحقن مطالبات تنزيل خبيثة (تنزيلات drive-by) في جلسة المتصفح الخاصة بك.

Q8: ما خطر مشاركة الملفات؟

إذا كانت مشاركة الملفات مفعّلة، يمكن لمستخدمين آخرين على الشبكة العامة قراءة دليل مجلداتك المحلي أو تعديله.

Q9: ما البوابة المقيّدة (captive portal)؟

صفحة تسجيل الدخول التي تستخدمها شبكات الفنادق أو المقاهي لمنح الوصول إلى الإنترنت، والتي قد ينتحلها المهاجمون أحيانًا.

Q10: هل يجب أن أوقف Wi-Fi عند عدم استخدامه؟

نعم، يمنع تعطيل Wi-Fi جهازك من الاتصال تلقائيًا بالشبكات غير الموثوقة.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء C)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q1: كيف يستغل هجوم الوسيط DNS؟

باستخدام انتحال DNS على موجّه مارق لتوجيه المتصفحات المستهدفة إلى صفحات هبوط تصيّد احتيالي مشابهة بدلًا من النطاقات المستهدفة.

Q2: ما اختطاف الجلسة؟

مهاجم يتنصت على ملف تعريف ارتباط جلسة غير مشفّر عبر Wi-Fi عامة ويستورده لتجاوز تسجيلات دخول بيانات الاعتماد.

Q3: ما تجريد SSL (SSL stripping)؟

هجوم الوسيط (MitM) الذي يخفّض فيه المهاجم طلب HTTPS الآمن للمستخدم إلى HTTP غير مشفّر، فيلتقط بيانات تسجيل الدخول كنص صريح.

Q4: كيف يحمي HSTS من تجريد SSL؟

يُلزم HTTP Strict Transport Security المتصفحات بالاتصال عبر HTTPS فقط، ويرفض الرجوع إلى HTTP غير المشفر. [3]

Q5: ما VPN ذو النفق المجزّأ؟

تهيئة توجّه حركة الشركة فقط عبر VPN وترسل بيانات الإنترنت العامة مباشرة، مما قد يعرّض لخطر كشف مسار التسرب.

نقطة التحقق 10: الأسئلة الشائعة المتقدمة حول الأمان (الجزء D)

استكشف الجوانب التقنية المتقدمة لأطر الأمان وتحليل البرمجيات الخبيثة والامتثال للبيانات.

Q6: لماذا يكون WPA2 عرضة لهجوم KRACK؟

يستغل هجوم Key Reinstallation Attack المصافحة الرباعية في WPA2 لفك تشفير الحزم دون كلمة مرور Wi-Fi.

Q7: ما عزل العميل (client isolation)؟

إعداد أمان في الموجّه يمنع أجهزة Wi-Fi المتصلة من التواصل المباشر فيما بينها، مما يحظر التنصت المحلي.

Q8: كيف يستخدم المهاجمون خوادم DNS مزيفة؟

يضبطون موجّهات خبيثة لتعيين خوادم DNS مزيفة للعملاء، مما يتيح لهم اعتراض جميع عمليات البحث على الويب وإعادة كتابتها.

Q9: هل يمكن لـ VPN إخفاء عنوان MAC المحلي لدي؟

لا. فعناوين MAC معرّفات محلية على الطبقة 2؛ استخدم بدلًا من ذلك إعداد العشوائية المدمج في MAC بجهازك (العنوان الخاص).

Q10: ما هجوم انتحال البوابة المقيّدة؟

مهاجم يستضيف بوابة مصادقة مزيفة على نقطة اتصال مارقة لسرقة بيانات الاعتماد تحت ستار الوصول المجاني إلى Wi-Fi.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

غالبًا ما يستخدم العاملون عن بُعد شبكات Wi-Fi في المقاهي والفنادق والمطارات، حيث لا يمكنهم التحكم في أمان الشبكة.

2. نظرة على الأمن

يمكن لنقطة الاتصال المارقة Evil Twin نسخ الاسم وعنوان MAC نفسيهما لشبكة موثوقة، مما يربك الأجهزة.

3. نظرة على الأمن

برامج التقاط الحزم مثل Wireshark مجانية ويمكنها عرض كلمات مرور HTTP غير المشفرة بنص صريح.

4. نظرة على الأمن

يستخدم أمان WPA3 المصادقة المتزامنة بين الأنداد (SAE) للحماية من هجمات القوة الغاشمة المحلية.

5. نظرة على الأمن

تتجاوز هجمات تجريد SSL حمايات HTTPS الأساسية باعتراض عمليات إعادة توجيه HTTP الأولية عند البوابة.

6. نظرة على الأمن

تمنع ترويسات الاستجابة HTTP Strict Transport Security (HSTS) المتصفحات من الرجوع إلى اتصالات HTTP غير المشفرة. [3]

7. رؤية حول الأمان

يمنع إيقاف 'الاتصال التلقائي' الهواتف الذكية من الاتصال بشبكات خبيثة مشابهة في الأماكن العامة.

8. رؤية حول الأمان

تفرض إعدادات VPN «الدائم التشغيل» في المؤسسات تمرير كل حركة مرور العاملين عن بُعد عبر جدران حماية الشركة.

9. رؤية حول الأمان

يمكن لنقاط الوصول المارقة تقديم إجابات DNS مزورة، تعيد توجيه النطاقات المستهدفة إلى خوادم تصيّد احتيالي.

10. نظرة على الأمن

من دون VPN، يستطيع المستخدمون الآخرون على نقطة اتصال مفتوحة رؤية المواقع والخوادم التي يتصل بها جهازك.

المراجع والمصادر التقنية

أُعد دليل الدراسة والألغاز التفاعلية استنادًا إلى معايير NIST وOWASP العالمية ومعايير الامتثال لخصوصية البيانات.

المراجع الأكاديمية والصناعية

[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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هو هجوم الوسيط (MitM)؟ → اعتراض الاتصالات بين طرفين وتعديلها على شبكة مشتركة

2 السؤال 2 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هي نقطة الوصول المارقة (التوأم الشرير)؟ → نقطة Wi-Fi خبيثة مهيأة بالـ SSID نفسه لشبكة شرعية

3 السؤال 3 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

كيف يحمي VPN حركة Wi-Fi العامة؟ → يغلّف جميع حزم الشبكة في نفق مشفّر، فتصبح غير مقروءة لأدوات التنصت

4 السؤال 4 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما هو التنصت على الحزم؟ → استخدام أدوات عتادية أو برمجية لالتقاط حزم الشبكة وتسجيلها

5 السؤال 5 — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما دور HTTPS؟ → تشفير حركة الجلسة بين المتصفح وخادم الويب

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يستطيع المستخدمون المتصلون التقاط البيانات النصية العادية بسهولة على شبكات Wi-Fi العامة المفتوحة.

7 السؤال 7

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: التوأم الشرير (Evil Twin) نقطة اتصال غير مصرح بها ينشئها مهاجم لمحاكاة نقطة حقيقية.

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يشفّر VPN الحركة في نفق، لذا لا تستطيع أدوات الاعتراض المحلية قراءتها.

9 السؤال 9

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يشفّر HTTPS تبادل HTTP بالكامل، بما في ذلك مسار URL ومحتوى الصفحة.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

توفر نقاط Wi-Fi الساخنة التي تستخدم أمان WPA3 حماية أقوى من الشبكات المفتوحة بلا كلمة مرور.

مفاتيح المفردات ومعيار التقييم

معيار التصحيح للمعلم: امنح 1 نقطة لكل مطابقة صحيحة (المجموع 8 نقطة) ولكل مصطلح سياق (المجموع 6 نقطة).

نقطة التحقق 4: مفتاح الإجابة – مطابقة المفاهيم

E 1. الاعتراض	F 2. التنصت	D 3. التوأم الشرير	H 4. HTTPS
G 5. VPN	B 6. النفق	A 7. WPA3	C 8. جدار الحماية

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 اعتراض	2 التنصت	3 التوأم الشرير	4 HTTPS
5 VPN	6 النفق		

نقطة التحقق 6 – نشاط بديل: مفتاح الإجابة – مطابقة المفردات

1 G – المعيار	2 C – التوام	3 B – التنصت	4 F – النفق
5 H – جدارحماية	6 A – الاعتراض	7 E – شبكةخاصة	8 D – الامن

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح الاعتراض والتنصت والتوأم الشرير بكلماتهم الخاصة وإعطاء مثال على كل منها.

دراسات الحالة:
اطلب من الطلاب أن يدعموا توصياتهم بحقائق من ورقة العمل لا بآرائهم.

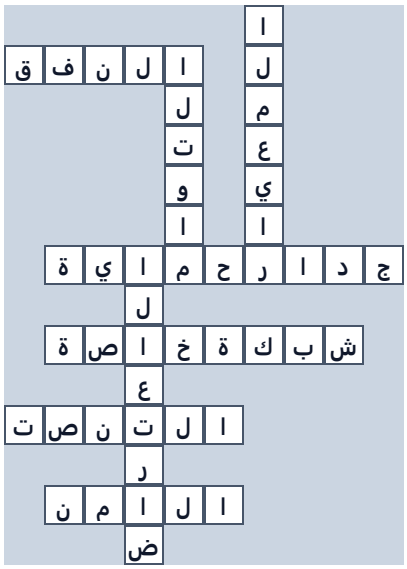
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات

ت	م	م	س	د	ف	ل	ط	ك	ض	ك	ف	ت	ه	م
ن	ح	ا	ص	ش	ب	ا	ب	ا	ت	ق	ض	ص	ش	ة
ص	ض	و	ه	ص	ج	ل	ع	ش	ل	ج	س	ع	ع	ص
ك	ق	ت	ص	ت	ن	ت	ل	ا	ر	ع	م	ع	ك	ل
ة	م	ل	ه	ن	ج	ر	ت	م	ك	ف	ع	ز	م	ب
ص	ي	ا	ج	ن	د	خ	ا	و	ن	ت	خ	ي	ي	د
ا	س	ز	خ	ج	ا	ع	ج	ل	ل	م	ض	ق	ا	ت
خ	ه	ب	ا	خ	ر	ف	ج	ص	ا	ا	ا	ج	ف	ر
ة	ج	د	ر	س	ح	ج	ك	ع	ع	ح	ل	ج	س	م
ك	خ	ن	د	ل	م	ا	و	ح	ا	ا	ل	ت	ا	ق
ب	ع	ك	ه	ض	ا	ل	ك	ش	م	ه	م	ر	ت	ع
ش	ة	ب	د	م	ي	ن	ض	س	ا	ل	خ	ا	ه	ة
ة	س	ر	س	ع	ة	ف	ل	ش	ط	ط	ق	ر	ر	ض
ك	ل	ر	خ	ا	ف	ق	و	د	و	ب	ة	م	ة	ب
ر	ط	خ	ر	ش	ف	ك	ف	ي	ت	ط	خ	ة	د	ة

حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

2 أفقي: النفق مسار بيانات آمن أثناء النقل (5 حروف)

3 أفقي: جدارحماية تصفية الحركة الواردة (9 حروف)

5 أفقي: شبكةخاصة شبكة افتراضية مشفرة (8 حروف)

6 أفقي: التنصت التقاط حزم بيانات الشبكة (6 حروف)

7 أفقي: الامن نقل الويب المؤمن (5 حروف)

عمودي

1 عمودي: المعيار معيار حديث لأمان Wi-Fi (7 حروف)

2 عمودي: التوام نقطة اتصال مارقة تحاكي شبكة Wi-Fi (6 حروف)

4 عمودي: الاعتراض قراءة الحركة أثناء انتقالها (8 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. اعتارلضا — الاعتراض
2. ماتاول — التوام
3. ةبشخاةصك — شبكةخاصة
4. رليعاام — المعيار
5. نتتاصل — التنصت
6. ماانل — الامن
7. فقانل — النفق
8. ةحيجردماا — جدارحماية

مفتاح تحدي الشيفرة السرية

"شفر حركة الشبكات العامة بشبكة خاصة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: احتواء التقاط الحزم على شبكة Wi-Fi العامة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يلاحظ مدير مبيعات عن بُعد متصل بشبكة Wi-Fi عامة في المطار تسريب عدة رسائل بريد إلكتروني تجارية حساسة بعد وقت قصير من إرسالها كنص عادي.
- الاستراتيجية والحل الموصى بهما: فرض استخدام عميل VPN للمؤسسات على جميع محطات العمل عن بُعد. وفرض إضافات المتصفح التي تعمل عبر HTTPS فقط، وحظر البروتوكولات غير المشفرة (مثل HTTP وFTP) في جدار حماية العميل.

B دراسة الحالة 2: الدفاع ضد نقطة الاتصال الوهمية التوأم الشريرة

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: ينشر مهاجمون نقطة وصول لاسلكية مارقة باسم 'CoffeeShop_Guest' تحاكي نقطة اتصال مقهى شرعية، فيلتقطون حركة الشبكة من الضيوف غير المنتبهين.
- الاستراتيجية والحل الموصى بهما: دقّق عناوين MAC الخاصة بـ BSSID لنقاط الوصول للتحقق من أصالة الشبكة. وافرض التحقق من وضعية العميل لمنع الاتصال بالشبكات المفتوحة، وألزم باستخدام نقاط الاتصال الخلوية للأعمال الحساسة.