الاسم: _____ التاريخ: _____ الدرجة: _____

منع سرقة الهوية والأصول
دليل الأمان

تسرب بيانات الاعتماد، والمصادقة متعددة العوامل، ومراقبة الويب المظلم، وتنبيهات تجميد الائتمان، والهندسة الاجتماعية

نظرة تعليمية على منع سرقة الهوية

مرحبًا! ترشدك حزمة الأنشطة هذه عبر منع سرقة الهوية والتخفيف منها. ستستكشف تسرّبات بيانات الاعتماد والمصادقة متعددة العوامل ومراقبة الويب المظلم وتنبيهات تجميد الائتمان ودفاع الهندسة الاجتماعية.

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**

مؤمَّن
تشفير البيانات
معيار AES بطول 256 بت

متوافق
المعايير العالمية
أطر GDPR وCCPA

انعدام الثقة
سياسة الوصول
المصادقة متعددة العوامل

افتح دليل VPN.com للأمن السيبراني

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

خارطة طريقك لتعلّم حماية الهوية

- افهم مخاطر انكشاف بيانات الاعتماد في منتديات الشبكة المظلمة.
- طبّق المصادقة متعددة العوامل (MFA) وتنبيهات تجميد الائتمان.
- صمّم دفاعات أمنية للشركات ضد عمليات الاحتيال الموجّهة بالهندسة الاجتماعية.

تعليمات دليل سرقة الهوية

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 حماية الهوية. واختم بالنشاط الإضافي «فكّر بسرعة».

منع سرقة الهوية وتأمين الأصول (مقدمة)

تستغل سرقة الهوية بيانات الاعتماد المسرّبة وعمليات تسجيل الدخول الضعيفة للاستيلاء على الحسابات الشخصية وحسابات الشركات. ويشكّل نشر المصادقة متعددة العوامل (MFA) وتجميد الائتمان وماسحات الويب المظلم وأطر SPF/DKIM/DMARC دفاعًا حاسمًا ضد الانتحال الرقمي.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما الطريقة الرئيسية التي يستخدمها لصوص الهوية لسرقة بيانات تسجيل الدخول؟

- A. إرسال تنبيهات بريد إلكتروني مزيفة لخداع المستخدمين كي يدخلوا كلمات المرور في بوابات منتحلة
- B. الاستماع إلى البث الإذاعي قرب مكتب الشركة التابع للمستخدم
- C. إلغاء تجزئة قرص التخزين المحلي لخادم المستخدم
- D. فصل إعدادات النسخ الاحتياطي الخارجية للشبكة

2. ما ضابط الأمان الذي يوفر أقوى دفاع ضد تسريبات بيانات الاعتماد؟

- A. المصادقة متعددة العوامل باستخدام مفاتيح عتادية
- B. إنشاء كلمات مرور طويلة باستخدام صيغ المتصفح الافتراضية
- C. تغيير أسماء مستخدمي البريد الإلكتروني كل ستة أشهر
- D. حذف سجلات تصفح تتبع ملفات تعريف الارتباط المخزنة

3. ما الذي يمثل تجميد الائتمان؟

- A. قفل التقارير الائتمانية لمنع اللصوص من فتح قروض غير مصرّح بها
- B. حذف سجلات المعاملات المصرفية من قواعد البيانات
- C. تعطيل قارئات شريط بطاقات الائتمان المغناطيسي على الماسحات الضوئية
- D. تشفير أقراص قواعد البيانات المحلية أثناء التخزين

4. لماذا تفيد مراقبة الويب المظلم؟

- A. ينبّه المستخدمين إذا ظهرت بيانات اعتمادهم المسرّبة في قواعد بيانات غير مشروعة
- B. يمنع البرمجيات الخبيثة النشطة من العمل في بيئات العزل الافتراضية
- C. يسرّع توجيه المتصفح على الشبكات الافتراضية
- D. يحظر محاولات الوصول الخلفية إلى قاعدة البيانات عبر حقن SQL

5. ماذا تعني الهندسة الاجتماعية؟

- A. التلاعب بالناس لدفعهم إلى كشف بيانات الاعتماد السرية طواعيةً
- B. فحص منافذ خوادم الشركة بحثًا عن ثغرات أمنية نشطة
- C. نسخ ملفات قواعد بيانات النظام احتياطيًا إلى أقراص صلبة غير متصلة بالإنترنت
- D. توجيه حزم الشبكة عبر ثلاث عقد onion مشفرة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. لا تؤثر سرقة الهوية إلا على الحسابات الرقمية عبر الإنترنت، لا على البريد الورقي.

صحيح خطأ

7 سؤال 7

7. يجب فرض المصادقة متعددة العوامل (MFA) على جميع الحسابات الشخصية معظم هجمات روبوتات حشو بيانات الاعتماد.

صحيح خطأ

8 سؤال 8

8. يحظر تجميد الائتمان عمليات التحقق الائتماني لكنه يمنعك من الوصول إلى حسابك المصرفي.

صحيح خطأ

9 سؤال 9

9. تحمي مديرات كلمات المرور المستخدمين من التصيّد الاحتيالي برفضها ملء كلمات المرور تلقائيًا على النطاقات المنتحلة.

صحيح خطأ

10 سؤال 10

10. غالبًا ما تستخدم رسائل التصيّد الاحتيالي لغة عاجلة لإثارة ردود فعل عاطفية سريعة.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يستهدف لصوص الهوية كلمات المرور الشخصية وكذلك _____ الخاصة بالمستخدمين.
2. ينبه إشعار المستخدمين بخروقات قواعد البيانات إلى _____ الحسابات الخاصة.
3. يسمى طلب رمز مؤقت لتسجيل الدخول _____ .
4. يسمى البحث في منتديات القراصنة عن بيانات مسروقة _____ الويب المظلم.
5. يتطلب منع الاستعلامات الائتمانية غير المصرح بها إجراء _____ للسجل الائتماني.
6. يبني تدريب الموظفين على الوعي بالتصيد الاحتيالي خط _____ الأمني الفعال.

بنك كلمات المفردات

الانتحال التجميد التصيد الدفاع المصادقة متعددة العوامل بيانات الاعتماد تسريبات مراقبة

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

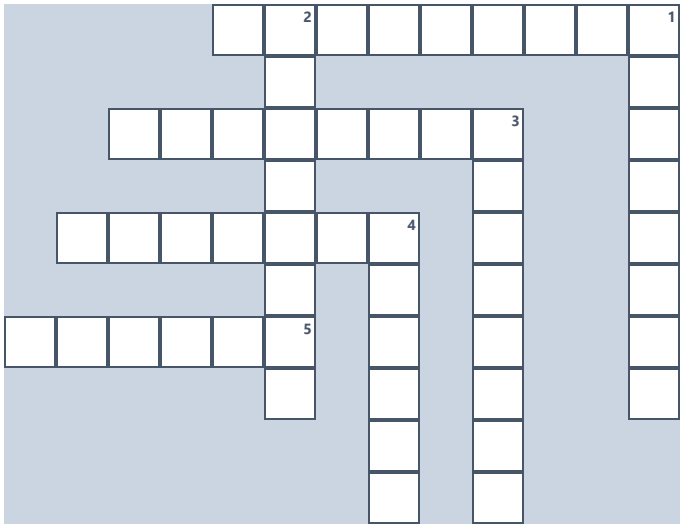
مطابقة التعريفات

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

1. بيانات الاعتماد	A	خطوة تحقق ثانوية (مثل مفاتيح الأجهزة) تحمي تسجيل الدخول إلى الحسابات.
2. التسريبات	B	إنشاء موقع ويب أو بريد إلكتروني مزيف لتقليد منظمة شرعية.
3. MFA	C	تقييد الوصول إلى ملفات الائتمان لمنع طلبات القروض الاحتيالية.
4. المراقبة	D	كشف غير مصرح به لقواعد بيانات خاصة تحتوي على سجلات مستخدمين شخصية.
5. التجميد	E	التدريب والضوابط التقنية المستخدمة للحماية من سرقة الهوية.
6. الدفاع	F	إرسال رسائل احتيالية لخداع المستخدمين لتسليم بيانات اعتمادهم.
7. الانتحال	G	مسح المنتديات عبر الإنترنت وقنوات المخترقين بحثًا عن بيانات الشركة المسروقة.
8. التصيّد الاحتيالي	H	أسماء المستخدمين وكلمات المرور والرموز المميزة الخاصة المستخدمة لمصادقة الهويات الرقمية.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

1. كشف غير مصرح به لقواعد بيانات خاصة تحتوي على سجلات المستخدمين الشخصية (9)

3. خطوة تحقق ثانوية (مثل مفاتيح الأجهزة) تحمي تسجيل الدخول إلى الحسابات (8)

4. تقييد الوصول إلى الملفات الائتمانية لمنع طلبات القروض الاحتيالية (7)

5. إرسال رسائل احتيالية لخداع المستخدمين وحملهم على تسليم بيانات الدخول (6)

عمودي

1. إنشاء موقع أو بريد مزيف لمحاكاة مؤسسة مشروعة (8)

2. أسماء المستخدمين وكلمات المرور والرموز الخاصة المستخدمة لمصادقة الهويات الرقمية (8)

3. فحص المنتديات وقنوات القراصنة بحثا عن بيانات مؤسسية مسروقة (8)

4. التدريب والضوابط التقنية المستخدمة للحماية من سرقة الهوية (6)

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

1 أفقي: كشف غير مصرح به لقواعد بيانات خاصة تحتوي على سجلات المستخدمين الشخصية (9 حروف):

3 أفقي: خطوة تحقق ثانوية (مثل مفاتيح الأجهزة) تحمي تسجيل الدخول إلى الحسابات (8 حروف):

4 أفقي: تقييد الوصول إلى الملفات الائتمانية لمنع طلبات القروض الاحتيالية (7 حروف):

5 أفقي: إرسال رسائل احتيالية لخداع المستخدمين وحملهم على تسليم بيانات الدخول (6 حروف):

عمودي

1 عمودي: إنشاء موقع أو بريد مزيف لمحاكاة مؤسسة مشروعة (8 حروف):

2 عمودي: أسماء المستخدمين وكلمات المرور والرموز الخاصة المستخدمة لمصادقة الهويات الرقمية (8 حروف):

3 عمودي: فحص المنتديات وقنوات القراصنة بحثا عن بيانات مؤسسية مسروقة (8 حروف):

4 عمودي: التدريب والضوابط التقنية المستخدمة للحماية من سرقة الهوية (6 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.

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

قائمة كلمات المفردات

الاعتماد التسريبات المصادقة المراقبة التجميد الدفاع الانتحال التصيد

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. الاعتماد
B. التسريبات
C. المصادقة
D. المراقبة
E. التجميد
F. الدفاع
G. الانتحال
H. التصيد

التعريفات وحقول المطابقة
1. إرسال رسائل احتيالية لخداع المستخدمين وحملهم على تسليم بيانات الدخول.
2. أسماء المستخدمين وكلمات المرور والرموز الخاصة المستخدمة لمصادقة الهويات الرقمية.
3. إنشاء موقع أو بريد مزيف لمحاكاة مؤسسة مشروعة.
4. التدريب والضوابط التقنية المستخدمة للحماية من سرقة الهوية.
5. فحص المنتديات وقنوات القراصنة بحثا عن بيانات مؤسسية مسروقة.
6. تقييد الوصول إلى الملفات الائتمانية لمنع طلبات القروض الاحتيالية.
7. كشف غير مصرح به لقواعد بيانات خاصة تحتوي على سجلات المستخدمين الشخصية.
8. خطوة تحقق ثانوية (مثل مفاتيح الأجهزة) تحمي تسجيل الدخول إلى الحسابات.

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. اعتامل دا _____
2. صاةلق دام _____
3. جامدتيل _____
4. نالحتالا _____
5. برلتيسات _____
6. بةرقالم _____
7. االفعدل _____
8. تدايصل _____

نشاط إضافي: فكّر بسرعة

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

1	أشياء تفعلها إذا سُرقت هويتك		
2	أشياء لا تشاركها على وسائل التواصل الاجتماعي		
3	أشياء تحتفظ بنسخة احتياطية منها		
4	بطاقات أو هويات في محفظتك		
5	مستندات ينبغي أن تحميها		
6	أشياء تفعلها بعد تسرّب البيانات		
7	أسباب لتحديث البرامج		
8	معلومات يريدها منتحل الهوية		
9	أجهزة يمكن اختراقها		
10	أماكن يمكن أن تتسرب منها بياناتك		
11	عادات آمنة يمكنك البدء بها اليوم		
12	علامات إصابة الحاسوب		
13	طرق لإثبات هويتك		
14	علامات سرقة الهوية		
15	علامات تحذيرية في البريد الإلكتروني		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: الحماية من انتحال هوية التنفيذيين



السيناريو: استُهدف مسؤول تنفيذي بارز في الإدارة العليا بأسماء نطاقات تستغل الأخطاء الإملائية وتحاكي بريده الإلكتروني الشخصي لخداع العملاء. صمّم خطة لحماية العلامة التجارية.

سؤال للنقاش: حلّل مخاطر انتحال العلامة التجارية، وفصّل ضوابط SPF/DKIM/DMARC والمصادقة.

دراسة الحالة 2: انكشاف بيانات اعتماد الشركة على الويب المظلم



السيناريو: يحتوي تسريب قاعدة بيانات من الشبكة المظلمة على عدة مئات من بيانات اعتماد الشركة العائدة لمديري أنظمة مؤسسة. صمّم استراتيجية للحد من الأثر.

سؤال للنقاش: لخّص عملية تنظيف بيانات الاعتماد، وخطّط لطرح مدير كلمات المرور.

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

29	28	24	21	10	23	1		22	3	28	27	26		24	6	1

29	8	8	18	3	24	23	1		29	21	8	1	14	24	23	1	2

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: ما سرقة الهوية؟

جريمة يسرق فيها المهاجم سجلات شخصية (مثل كلمات المرور أو أرقام الضمان الاجتماعي) لانتحال شخصية آخر لتحقيق مكسب مالي.

Q2: ما السبب الأكثر شيوعًا لسرقة الهوية؟

التصيّد الاحتيالي من أبرز الطرق التي يحصل بها اللصوص على كلمات المرور، إذ يستدرج المستخدمين إلى مواقع ويب مزيفة منتحلة.

Q3: كيف تحمي المصادقة متعددة العوامل (MFA) الهويات؟

تتطلب المصادقة متعددة العوامل (MFA) إثباتًا ثانيًا (مثل مفتاح عتادي) لتسجيل الدخول، فتحجب المهاجمين حتى لو سرقوا كلمة مرورك.

Q4: ما تجميد الائتمان؟

خدمة مجانية تمنع مكاتب الائتمان من مشاركة ملفك الائتماني، فتوقف اللصوص عن فتح قروض جديدة باسمك. [2]

Q5: ما مراقبة الويب المظلم؟

برنامج يفحص منتديات المخترقين بحثًا عن رسائل البريد الإلكتروني وكلمات المرور والسجلات الشخصية المسرّبة، وينبهك إذا انكشفت بياناتك.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ماذا تعني حشو بيانات الاعتماد (credential stuffing)؟

روبوتات آلية تختبر قوائم كلمات المرور المسرّبة عبر مئات المواقع للاستيلاء على الحسابات النشطة.

Q7: لماذا يُعد انتحال البريد الإلكتروني خطيرًا؟

يتيح للمهاجمين انتحال اسم المرسل في رسائل البريد الإلكتروني، فتبدو رسائل التصيّد الاحتيالي كأنها من زملاء موثوقين.

Q8: كيف توقف مديرات كلمات المرور سرقة الهوية؟

تخزّن كلمات مرور معقدة وفريدة لكل حساب وترفض ملء بيانات الاعتماد تلقائيًا في نطاقات التصيّد المزيفة.

Q9: ما التصيّد الموجَّه (spear phishing)؟

هجوم تصيّد احتيالي موجَّه للغاية يُخصَّص باسم الضحية وتفاصيله لزيادة احتمال الخداع.

Q10: ما الفرق بين تنبيه الائتمان وتجميده؟

ينبّه التنبيه المقرضين إلى التحقق من هويتك قبل فتح الحسابات، بينما يحظر التجميد الوصول إلى ملفك الائتماني بالكامل. [2]

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

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

Q1: كيف يؤدي تبديل شريحة SIM إلى سرقة الهوية؟

يقنع المهاجمون موظفي شركة الاتصالات بنقل رقم هاتف الضحية إلى شريحة SIM جديدة، فيستولون على رموز المصادقة الثنائية 2FA المرسلة عبر الرسائل النصية.

Q2: ما دور DMARC في منع سرقة الهوية؟

يتيح DMARC لأصحاب النطاقات منع وصول رسائل البريد المنتحلة إلى صناديق الوارد، ما يوقف الرسائل المزيفة التي تحاكي نطاقات الشركات.

Q3: لماذا يصعب اكتشاف سرقة الهوية الاصطناعية؟

يجمع اللصوص أرقام SSN حقيقية مع أسماء وتواريخ ميلاد مزيفة لبناء ملفات ائتمانية جديدة تمامًا، متجاوزين تنبيهات الاحتيال الأساسية.

Q4: كيف يستغل سماسرة البيانات الهويات الشخصية؟

يجمع الوسطاء السجلات العامة وسلوك الويب وسجلات المشتريات لتجميع ملفات تعريفية شاملة، يمكن تسريبها أو بيعها.

Q5: لماذا تُعد المصادقة متعددة العوامل عبر الرسائل النصية SMS معرّضة للاختراق؟

حركة الرسائل القصيرة SMS عرضة للاعتراض والتصيّد الاحتيالي وهجمات تبديل شريحة SIM على مستوى شركة الاتصالات.

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

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

Q6: ما قفل ملف الائتمان؟

خدمة تجارية مشابهة للتجميد، تتيح للمستخدمين فتح ملفهم الائتماني أو قفله فورًا عبر تطبيق الجوال.

Q7: كيف تغذي اختراقات بيانات الشركات سرقة الهوية؟

تكشف قواعد البيانات المسرّبة ملايين بيانات الاعتماد النصية الصريحة، فتمنح اللصوص البيانات الخام اللازمة لتنفيذ احتيال موجّه لانتحال الهوية.

Q8: ما خطر الإفراط في المشاركة على وسائل التواصل الاجتماعي؟

يمنح نشر أسماء الحيوانات الأليفة وأماكن الميلاد وأسماء عائلات الأمهات قبل الزواج علنًا اللصوص إجابات أسئلة استرداد الحسابات الشائعة.

Q9: كيف يحمي تسجيل الدخول البيومتري ملفات الهوية؟

تربط القياسات الحيوية تسجيلات الدخول بسمات مثل بصمات الأصابع أو الوجوه؛ وعند حفظها على الجهاز يصعب سرقتها، لكن البيانات الحيوية المخزّنة قد تتسرب.

Q10: كيف تكافح قاعدة العلامات الحمراء سرقة الهوية؟

لائحة اتحادية تُلزم المؤسسات المالية بوضع برامج مكتوبة لاكتشاف علامات التحذير من سرقة الهوية والاستجابة لها.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

يتيح موقع IdentityTheft.gov، الذي تديره لجنة التجارة الفيدرالية (FTC)، لضحايا سرقة الهوية في الولايات المتحدة الإبلاغ عنها والحصول على خطة تعافٍ شخصية. [1]

2. نظرة على الأمن

مفاتيح الأمان المادية هي مصادقة متعددة العوامل (MFA) مقاومة للتصيّد، وهي أقوى أنواع MFA التي تحث عليها CISA. [4]

3. نظرة على الأمن

كلمات المرور المخترقة نقطة دخول شائعة في اختراقات البيانات، وتغذي الاحتيال على الهوية لاحقًا.

4. نظرة على الأمن

تجميد الائتمان مجاني بموجب القانون الاتحادي، ويمنع المقرضين من الاطلاع على الملفات الائتمانية إلى أن يُفتح. [2]

5. نظرة على الأمن

يتيح DMARC لأصحاب النطاقات إبلاغ خوادم البريد برفض رسائل البريد المنتحلة التي تفشل في الفحوص أو عزلها. [7]

6. نظرة على الأمن

يتيح تبديل شريحة SIM للمخترقين تجاوز المصادقة الثنائية القائمة على الرسائل القصيرة SMS في بوابات البنوك.

7. رؤية حول الأمان

يمزج احتيال الهوية الاصطناعية بين تفاصيل حقيقية ومزيفة، مما يصعّب على المقرضين اكتشافه.

8. رؤية حول الأمان

يعيد كثير من الناس استخدام كلمة المرور نفسها عبر حساباتهم على الإنترنت، لذا قد يكشف اختراق واحد عدة حسابات منها.

9. رؤية حول الأمان

يجمع وسطاء البيانات ملفات مفصلة عن أعداد كبيرة من المستهلكين، ما يخلق مخاطر مركّزة على الخصوصية.

10. نظرة على الأمن

قد يستغرق التعافي من سرقة الهوية شهورًا من العمل، مثل الاعتراض على الرسوم وتصحيح تقارير الائتمان.

المراجع والمصادر التقنية

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

المراجع الأكاديمية والصناعية

[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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 السؤال 1 — الإجابة الصحيحة: A

ملاحظة للمعلم

ما الطريقة الرئيسية التي يستخدمها لصوص الهوية لسرقة بيانات تسجيل الدخول؟ → إرسال تنبيهات بريد إلكتروني مزيفة لخداع المستخدمين كي يدخلوا كلمات المرور في بوابات منتحلة

2 السؤال 2 — الإجابة الصحيحة: A

ملاحظة للمعلم

ما ضابط الأمان الذي يوفر أقوى دفاع ضد تسريبات بيانات الاعتماد؟ → المصادقة متعددة العوامل باستخدام مفاتيح عتادية

3 السؤال 3 — الإجابة الصحيحة: A

ملاحظة للمعلم

ما الذي يمثل تجميد الائتمان؟ → قفل التقارير الائتمانية لمنع اللصوص من فتح قروض غير مصرّح بها

4 السؤال 4 — الإجابة الصحيحة: A

ملاحظة للمعلم

لماذا تفيد مراقبة الويب المظلم؟ → ينبّه المستخدمين إذا ظهرت بيانات اعتمادهم المسرّبة في قواعد بيانات غير مشروعة

5 السؤال 5 — الإجابة الصحيحة: A

ملاحظة للمعلم

ماذا تعني الهندسة الاجتماعية؟ → التلاعب بالناس لدفعهم إلى كشف بيانات الاعتماد السرية طواعيةً

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يمكن أن تبدأ سرقة الهوية خارج الإنترنت أيضًا، مثل سرقة البريد أو المستندات.

7 السؤال 7

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

يحجب فرض المصادقة متعددة العوامل (MFA) على جميع الحسابات الشخصية معظم هجمات روبوتات حشو بيانات الاعتماد.

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

يوقف تجميد الائتمان عمليات التحقق الائتماني الجديدة لكنه لا يؤثر في حساباتك الحالية.

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تحمي مديرات كلمات المرور المستخدمين من التصيّد الاحتيالي برفضها ملء كلمات المرور تلقائيًا على النطاقات المنتحلة.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

غالبًا ما تستخدم رسائل التصيّد الاحتيالي لغة عاجلة لإثارة ردود فعل عاطفية سريعة.

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

H 1. بيانات الاعتماد	D 2. التسريبات	A 3. MFA	G 4. المراقبة
C 5. التجميد	E 6. الدفاع	B 7. الانتحال	F 8. التصيّد الاحتيالي

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 بيانات الاعتماد	2 تسريبات	3 المصادقة متعددة العوامل	4 مراقبة
5 التجميد	6 الدفاع		

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

1 H – التصيد	2 A – الاعتماد	3 G – الانتحال	4 F – الدفاع
5 D – المراقبة	6 E – التجميد	7 B – التسريبات	8 C – المصادقة

ملاحظات النقاش للمعلمين

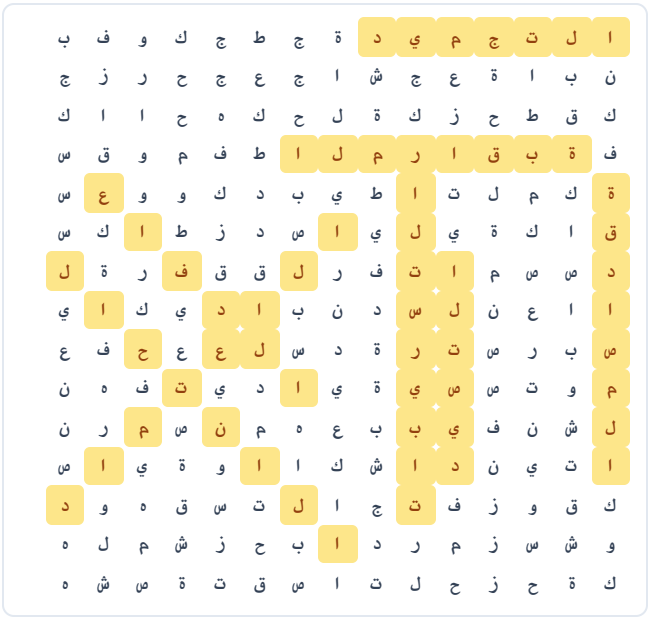
المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح بيانات الاعتماد والتسريبات وMFA بكلماتهم الخاصة وإعطاء مثال على كل منها.

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

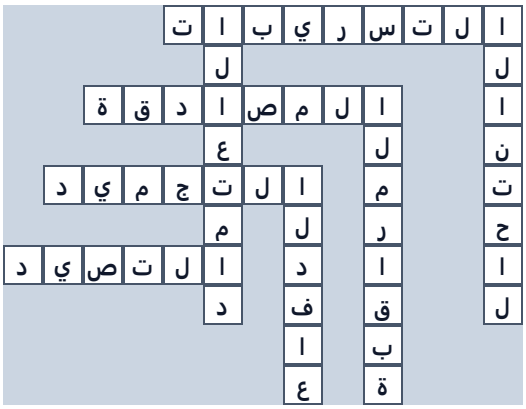
تقييم المصادر:
اطلب من الطلاب التحقق من ادعاء واحد على الأقل من مراجع ورقة العمل، وناقش لماذا قد تتغير الأرقام والأسعار والقواعد مع الوقت.

مفاتيح الألغاز وملاحظات المعلم

حل البحث عن الكلمات



حل الكلمات المتقاطعة



دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: التسريبات كشف غير مصرح به لقواعد بيانات خاصة تحتوي على سجلات المستخدمين الشخصية (9 حروف)

3 أفقي: المصادقة خطوة تحقق ثانوية (مثل مفاتيح الأجهزة) تحمي تسجيل الدخول إلى الحسابات (8 حروف)

4 أفقي: التجميد تقييد الوصول إلى الملفات الائتمانية لمنع طلبات القروض الاحتيالية (7 حروف)

5 أفقي: التصيد إرسال رسائل احتيالية لخداع المستخدمين وحملهم على تسليم بيانات الدخول (6 حروف)

عمودي

1 عمودي: الانتحال إنشاء موقع أو بريد مزيف لمحاكاة مؤسسة مشروعة (8 حروف)

2 عمودي: الاعتماد أسماء المستخدمين وكلمات المرور والرموز الخاصة المستخدمة لمصادقة الهويات الرقمية (8 حروف)

3 عمودي: المراقبة فحص المنتديات وقنوات القراصنة بحثا عن بيانات مؤسسية مسروقة (8 حروف)

4 عمودي: الدفاع التدريب والضوابط التقنية المستخدمة للحماية من سرقة الهوية (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. اعتاملدا	الاعتماد	5. برلتيسات	التسريبات
2. صاةلقدام	المصادقة	6. بةرقاالم	المراقبة
3. جامدتيل	التجميد	7. االفعدل	الدفاع
4. نالحتالا	الانتحال	8. تدايصل	التصيد

مفتاح تحدي الشيفرة السرية

"احم هويتك الرقمية بالمصادقة المتعددة"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: الحماية من انتحال هوية التنفيذيين

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: استُهدف مدير تنفيذي بارز بنطاقات تستغل الأخطاء الإملائية (typo-squatting) تحاكي بريده الشخصي لاحتيال العملاء. صمّم خطة لحماية العلامة التجارية.
- الاستراتيجية والحل الموصى بهما: سجّل جميع صيغ تهجئة اسم المدير التنفيذي الشائعة. ونفّذ بروتوكولات مصادقة البريد الإلكتروني (DMARC وDKIM وSPF) لمنع انتحال النطاق. وفرض المصادقة متعددة العوامل بالعتاد على جميع عمليات تسجيل الدخول لكبار المسؤولين التنفيذيين في الشركة.

B دراسة الحالة 2: انكشاف بيانات اعتماد الشركة على الويب المظلم

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: تحتوي نسخة قاعدة بيانات من الويب المظلم على عدة مئات من بيانات اعتماد الشركة العائدة لمسؤولي الأنظمة في مؤسسة. صمّم استراتيجية للحد من الأثر.
- الاستراتيجية والحل الموصى بهما: نفّذ إعادة تعيين كلمات المرور على مستوى الشركة. ألزم باستخدام مدير كلمات مرور مؤسسي. فعّل المصادقة متعددة العوامل (MFA) عبر جميع بوابات الأنظمة وأعدّ تنبيهات مراقبة آلية ومستمرة للويب المظلم.