الاسم: _____ التاريخ: _____ الدرجة: _____

الاحتيال عبر الإنترنت والهندسة الاجتماعية دليل الحماية

التصيّد الاحتيالي عبر البريد الإلكتروني، والنطاقات المنتحلة، والتصيّد الصوتي (vishing)، واحتيال الدعم، والتحقق خارج النطاق، واختراق البريد التجاري (BEC)

نظرة عامة على التعلّم: الاحتيال عبر الإنترنت

مرحبًا! ترشدك حزمة الأنشطة هذه عبر الدفاع ضد الاحتيال عبر الإنترنت. ستستكشف مواقع التصيّد الوهمية وأساليب الهندسة الاجتماعية واحتيال الدعم الفني ونواقل الاحتيال بالتحويلات المصرفية وطرق التحقق من الدفع.

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/online-scams/

خارطة طريقك لتعلّم الحماية من الاحتيال عبر الإنترنت

- تعرّف على المؤشرات الشائعة لعمليات احتيال الدعم الفني والنطاقات المقلّدة للأخطاء الإملائية (typosquatting).
- طبّق بروتوكولات التحقق من البريد الإلكتروني (SPF وDKIM وDMARC) ضد الانتحال.
- ضع آلية للتحقق من المعاملات خارج النطاق لمنع احتيال الحوالات في الأعمال.

تعليمات دليل الاحتيال عبر الإنترنت

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 الحماية من الاحتيال عبر الإنترنت. واختم بالنشاط الإضافي «فكّر بسرعة».

الحماية من الاحتيال عبر الإنترنت والهندسة الاجتماعية (مقدمة)

يستغل الاحتيال عبر الإنترنت السلوك البشري من خلال التصيّد الاحتيالي والنوافذ المنبثقة للدعم والتصيّد الصوتي والاحتيال بالحوالات. ويساعد فرض التحقق من المعاملات عبر قناة منفصلة وقواعد النطاق SPF/DKIM/DMARC على حظر ناقلات الهندسة الاجتماعية عند البوابة.

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

نقطة التحقق 1: تحدي الاختيار من متعدد

1. ما المؤشر الرئيسي على احتيال الدعم الفني؟
   - A. نافذة منبثقة تدّعي أن نظامك مصاب وتطالبك بالاتصال برقم هاتف
   - B. تحديث أمني آلي يُنزَّل من سجل رسمي
   - C. مدير كلمات مرور يرفض ملء بيانات الاعتماد على نطاق شركة
   - D. نسخ احتياطي للملفات يعمل في الخلفية على إعداد قرص خارجي

2. ما الأسلوب الذي يستخدم نطاقات مرسل منتحلة لسرقة بيانات الحسابات المصرفية؟
   - A. التصيّد الاحتيالي عبر البريد الإلكتروني
   - B. فحص المنافذ
   - C. حقن الذاكرة
   - D. التمزيق التشفيري

3. ما الذي يمثل احتيال التحويل المصرفي؟
   - A. خداع الضحايا لإرسال الأموال إلى حسابات شركات مزيفة باستخدام الهندسة الاجتماعية
   - B. تشفير قواعد بيانات النظام باستخدام حمولات برامج الفدية
   - C. الاستعلام عن قواعد البيانات عبر أوامر حقن SQL
   - D. نسخ ملفات النظام احتياطيًا إلى أقراص تخزين غير متصلة

4. لماذا ينشئ المحتالون مواقع تسوق مزيفة؟
   - A. لسرقة تفاصيل بطاقات الائتمان وبيانات اعتماد الدفع من المشترين
   - B. لاستضافة جداول قواعد بيانات تحليل البرمجيات الخبيثة المعزولة
   - C. لتسريع تسليم الطلبات عبر الإنترنت
   - D. لاختبار تصاميم المواقع الجديدة مجانًا

5. ماذا يعني التصيّد الصوتي (Vishing)؟
   - A. عمليات احتيال التصيّد الصوتي عبر شبكات الهاتف لسرقة بيانات الاعتماد
   - B. فحص الشبكات المحلية بحثًا عن أجهزة نظام غير مؤمّنة
   - C. استعادة قواعد بيانات النظام بعد اختراق غير مصرح به
   - D. تشغيل شيفرة غير موثوقة داخل حاويات افتراضية آمنة

نقطة التحقق 2: تحدي صحيح أم خطأ

6 سؤال 6

6. لا تستهدف عمليات التصيّد الاحتيالي سوى المستخدمين النهائيين، ولا تستهدف أهداف الحيتان التنفيذية أبدًا.

صحيح خطأ

7 سؤال 7

7. تستخدم النطاقات المنتحلة غالبًا أخطاء إملائية طفيفة (مثل amaz0n.com) لمحاكاة العلامات التجارية الموثوقة.

صحيح خطأ

8 سؤال 8

8. يمكن حل عمليات احتيال الدعم الفني بمنح المتصل وصولًا عن بُعد.

صحيح خطأ

9 سؤال 9

9. تستغل الهندسة الاجتماعية علم النفس البشري مثل الخوف والاستعجال لتجاوز قواعد الأمان.

صحيح خطأ

10 سؤال 10

10. ينبغي دائمًا التحقق من طلبات التحويل المصرفي عبر قنوات اتصال خارج النطاق.

صحيح خطأ

نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. تسمى رسائل البريد الاحتيالية التي تخدع المستخدمين _____ .
2. عناوين الويب التي تحاكي علامات موثوقة هي عناوين _____ .
3. يسمى الاحتيال عبر المكالمات الذي يستهدف تفاصيل البنك _____ .
4. النافذة المنبثقة التي تطالب بالمال لإزالة فيروس هي _____ للدعم الفني.
5. يتطلب تأكيد طلب دفع _____ عبر قناة خارج النطاق.
6. تسمى إعادة توجيه المعاملات التجارية إلى حسابات اللصوص احتيال _____ .

بنك كلمات المفردات

احتيال | التحقق | التحويل | التصيد الاحتيالي | التصيد الصوتي | الحيتان | النصية | منتحلة

اكتب إجاباتك هنا:

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

نقطة التحقق 4: مطابقة مفاهيم الأمان

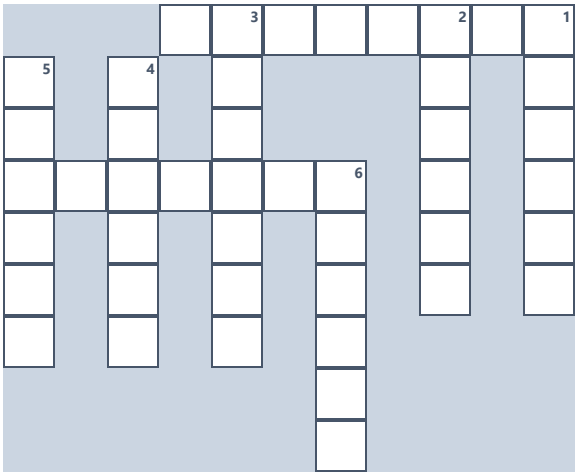
مطابقة التعريفات

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

1. التصيّد الاحتيالي	A	إعادة توجيه احتيالية للمعاملات المصرفية إلى حسابات إجرامية.
2. منتحَل	B	مخطط احتيالي يهدف إلى سرقة الأموال أو بيانات الدخول من الضحايا.
3. التصيّد الصوتي	C	إرسال رسائل نصية احتيالية لسرقة بيانات اعتماد الحسابات على الجوال.
4. احتيال	D	مكالمات صوتية احتيالية تهدف إلى سرقة بيانات الاعتماد وتفاصيل الحسابات.
5. التحقق	E	هجمات تصيّد احتيالي موجّهة تهدف إلى سرقة بيانات اعتماد المديرين التنفيذيين من الإدارة العليا.
6. التحويل المصرفي	F	عنوان بريد مرسل أو موقع ويب منتحل مصمم ليبدو شرعيًا.
7. صيد الحيتان	G	حملات بريد إلكتروني احتيالية تهدف إلى سرقة بيانات تسجيل الدخول وكلمات المرور.
8. التصيّد بالرسائل	H	تأكيد تفاصيل الدفع باستخدام وسيلة اتصال ثانوية موثوقة.

نقطة التحقق 5: لغز الكلمات المتقاطعة

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



أفقي

1. مخطط خادع يهدف إلى سرقة المال أو بيانات الدخول من الضحايا (8)

6. هجمات تصيد موجهة تستهدف سرقة بيانات الدخول من كبار المديرين التنفيذيين (7)

عمودي

1. تأكيد تفاصيل الدفع عبر وسيلة تواصل ثانوية موثوقة (6)

2. حملات بريد احتيالية مصممة لسرقة بيانات الدخول وكلمات المرور (6)

3. إعادة توجيه خادعة للمعاملات المصرفية إلى حسابات المجرمين (7)

4. عنوان مرسل أو موقع محاكى مصمم ليبدو مشروعا (6)

5. إرسال رسائل نصية احتيالية لسرقة بيانات دخول حسابات الجوال (6)

6. مكالمات صوتية احتيالية مصممة لسرقة بيانات الدخول وتفاصيل الحسابات (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: مخطط خادع يهدف إلى سرقة المال أو بيانات الدخول من الضحايا (8 حروف):

6 أفقي: هجمات تصيد موجهة تستهدف سرقة بيانات الدخول من كبار المديرين التنفيذيين (7 حروف):

عمودي

1 عمودي: تأكيد تفاصيل الدفع عبر وسيلة تواصل ثانوية موثوقة (6 حروف):

2 عمودي: حملات بريد احتيالية مصممة لسرقة بيانات الدخول وكلمات المرور (6 حروف):

3 عمودي: إعادة توجيه خادعة للمعاملات المصرفية إلى حسابات المجرمين (7 حروف):

4 عمودي: عنوان مرسل أو موقع محاكى مصمم ليبدو مشروعا (6 حروف):

5 عمودي: إرسال رسائل نصية احتيالية لسرقة بيانات دخول حسابات الجوال (6 حروف):

6 عمودي: مكالمات صوتية احتيالية مصممة لسرقة بيانات الدخول وتفاصيل الحسابات (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.

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

قائمة كلمات المفردات

التصيد | منتحلة | الصوتي | الاحتيال | التحقق | التحويل | الحيتان | النصية

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	التعريفات وحقول المطابقة
A. التصيد	1. عنوان مرسل أو موقع محاكى مصمم ليبدو مشروعا.
B. منتحلة	2. تأكيد تفاصيل الدفع عبر وسيلة تواصل ثانوية موثوقة.
C. الصوتي	3. إعادة توجيه خادعة للمعاملات المصرفية إلى حسابات المجرمين.
D. الاحتيال	4. إرسال رسائل نصية احتيالية لسرقة بيانات دخول حسابات الجوال.
E. التحقق	5. هجمات تصيد موجهة تستهدف سرقة بيانات الدخول من كبار المديرين التنفيذيين.
F. التحويل	6. مكالمات صوتية احتيالية مصممة لسرقة بيانات الدخول وتفاصيل الحسابات.
G. الحيتان	7. حملات بريد احتيالية مصممة لسرقة بيانات الدخول وكلمات المرور.
H. النصية	8. مخطط خادع يهدف إلى سرقة المال أو بيانات الدخول من الضحايا.

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. ت ا ص ي د ل
2. ي ا ص ت و ل
3. ا ت ح ق ق ل
4. ن ل ت ي ا ا ح
5. ح ت ة م ل ن
6. ا ل ح ي ا ت ل ا
7. ا ي و ل ل ح ت
8. ن ة ا ي ص ل

نشاط إضافي: فكّر بسرعة

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

1	أجهزة يمكن اختراقها		
2	عبارات يستخدمها المحتالون كثيرًا		
3	طرق دفع يطلبها المحتالون		
4	أنواع الاحتيال عبر الإنترنت		
5	عروض أفضل من أن تكون حقيقية		
6	أماكن للإبلاغ عن الاحتيال		
7	كلمات متعلقة بالأمن السيبراني		
8	أشخاص يمكنك تحذيرهم من الاحتيال		
9	أشياء تحتفظ بنسخة احتياطية منها		
10	علامات تحذيرية في البريد الإلكتروني		
11	علامات إصابة الحاسوب		
12	طرق للتحقق من متجر إلكتروني		
13	طرق لحماية حساباتك		
14	أشياء تفعلها إذا تعرضت للاحتيال		
15	أشياء تفعلها بعد تسرّب البيانات		

نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

دراسة الحالة 1: منع احتيال التحويلات البنكية في الشركات



السيناريو: يتلقى قسم المالية بريدًا إلكترونيًا عاجلًا من عنوان مورّد منتحَل، يطلب توجيه تحويلات الفواتير المستقبلية إلى رقم توجيه جديد.

سؤال للنقاش: لخّص سياسة التحقق من الاحتيال في التحويلات المصرفية، وحدّد ضوابط مصادقة البريد الإلكتروني.

دراسة الحالة 2: حادثة تصيّد احتيالي لصيد الحيتان على التنفيذيين



السيناريو: نقر مسؤول تنفيذي على رابط تصيّد احتيالي يدّعي احتواءه على مستند اجتماع مجلس إدارة آمن، وأدخل بيانات اعتماد شركته الأساسية على بوابة منتحَلة.

سؤال للنقاش: فصّل خطوات الاستجابة للحوادث، واشرح كيفية تدقيق عمليات تسجيل دخول المسؤول التنفيذي.

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

8	28	14	3	23	1		3	1	23	24	6		20	13	3	22	1
6	12	1	24		10	2	18		21	21	6	3	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 الاحتيال عبر الإنترنت؟

مخطط احتيالي يستخدم القنوات الرقمية لخداع الضحايا كي يرسلوا الأموال أو يكشفوا بيانات اعتمادهم الشخصية.

Q2: ما المؤشر الرئيسي على التصيّد الاحتيالي عبر البريد الإلكتروني؟

رسالة تدّعي الاستعجال (مثل تعليق الحساب) وتوجّهك إلى رابط لا يطابق النطاق الرسمي.

Q3: ما انتحال أسماء النطاقات بالأخطاء الإملائية (typosquatting)؟

تسجيل نطاقات تحتوي أخطاء إملائية شائعة للعلامات التجارية الشهيرة (مثل amaz0n.com) لاستضافة مواقع تصيّد احتيالي مزيفة.

Q4: ما احتيال الدعم الفني؟

نافذة منبثقة تدّعي أن حاسوبك مصاب، وتوجّهك إلى الاتصال برقم ودفع ثمن برنامج تنظيف مزيف أو خدمات وصول عن بُعد. [1]

Q5: ما التصيّد الصوتي (vishing)؟

هجمات تصيّد احتيالي تستخدم المكالمات الهاتفية الصوتية لخداع الضحايا لتقديم تفاصيل الحساب المصرفي أو تسجيل الدخول.

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

Q6: ماذا يعني الاحتيال عبر التحويلات المصرفية (wire fraud)؟

إعادة توجيه معاملات الدفع إلى حسابات احتيالية عن طريق انتحال صفة الموردين أو المديرين التنفيذيين.

Q7: ما صيد الحيتان (whaling)؟

شكل موجَّه للغاية من التصيّد الموجَّه يستهدف مباشرة أهدافًا عالية القيمة مثل كبار المديرين التنفيذيين.

Q8: ما التصيّد عبر الرسائل النصية (smishing)؟

رسائل نصية احتيالية تُرسل إلى الأجهزة المحمولة وتتضمن روابط تقود إلى بوابات مزيفة أو تحديثات تتبع.

Q9: لماذا يُعد التحقق خارج النطاق بالغ الأهمية؟

يؤكد تفاصيل المعاملة عبر قناة اتصال منفصلة (مثل مكالمة هاتفية)، متجنبًا سلاسل البريد الإلكتروني المخترَقة.

Q10: كيف تعمل عملية احتيال حساب الضمان المزيف؟

ينشئ المحتالون موقع حساب ضمان منتحلًا، ويزعمون أن الأموال محتجزة بأمان، ثم يسرقون الإيداع المحوَّل من المشتري.

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

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

Q1: كيف يستخدم المحتالون اختراق البريد الإلكتروني للأعمال (BEC) لتنفيذ احتيال الحوالات؟

يستولون على حساب البريد الإلكتروني لموظف شرعي، ويراقبون سلاسل الفواتير، ويرسلون بيانات فوترة محدّثة بحسابات مصرفية احتيالية.

Q2: ما خطر هجمات التماثل الحرفي في أسماء النطاقات الدولية (IDN) ضمن الاحتيال عبر الإنترنت؟

استخدام أحرف غير ASCII تبدو مطابقة للحروف العادية (مثل الحرف السيريلي 'a') لتسجيل نطاقات منتحلة تحاكي علامات تجارية حقيقية.

Q3: لماذا يُعد فحص ترويسة البريد الإلكتروني مهمًا في اكتشاف الاحتيال؟

يكشف عنوان IP الفعلي لخادم المصدر وحالة التحقق من SPF/DKIM، ما يبيّن ما إذا كان نطاق المرسل مزوّرًا.

Q4: كيف يستغل محتالو الدعم الفني برامج سطح المكتب البعيد؟

يستخدمون أدوات مثل AnyDesk أو TeamViewer للاتصال بجهاز الضحية وزرع برمجيات خبيثة وسرقة كلمات المرور المحفوظة.

Q5: ما هدف عمليات احتيال الرسوم المسبقة؟

خداع الضحايا لدفع رسوم معالجة مقدمًا مقابل مكافأة مالية كبيرة غير موجودة.

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

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

Q6: كيف يستخدم المحتالون التنميط عبر وسائل التواصل الاجتماعي في التصيّد الاحتيالي الموجَّه؟

يجمعون الهياكل التنظيمية للشركات وأسماء الموظفين لصياغة رسائل تصيّد موجّه مقنعة.

Q7: لماذا تقدم متاجر الويب المزيفة خصومات كبيرة؟

لإغراء المشترين بإدخال بيانات بطاقاتهم الائتمانية، واقتناص بيانات الاعتماد لإعادة استخدامها أو بيعها في منتديات بطاقات الائتمان المسروقة.

Q8: كيف تحظر سجلات DMARC عمليات التصيّد الاحتيالي؟

يتيح DMARC لأصحاب النطاقات أن يطلبوا من المستقبلين عزل الرسائل التي تفشل في فحوص SPF وDKIM المتوافقة أو رفضها، ما يحجب الانتحال المباشر. [5]

Q9: ما تهديد بوابات حصاد بيانات الاعتماد؟

صفحات هبوط منتحلة مصممة لتبدو تمامًا مثل Microsoft 365 أو مساحات عمل Google، وتسرق بيانات تسجيل الدخول أثناء إدخالها.

Q10: كيف تبلّغ فرق الأمان عن نطاقات الاحتيال وتعطّلها؟

بتقديم أدلة الاحتيال إلى البريد الإلكتروني لإساءة الاستخدام لدى المسجّل ومزود الاستضافة وسجل Google Safe Browsing.

الجزء 11: 10 حقائق ورؤى واقعية عن الأمن السيبراني

راجع حقائق واقعية عن الاختراقات الأمنية وآليات الدفاع ومعايير الامتثال.

1. نظرة على الأمن

كان التصيّد الاحتيالي والانتحال أكثر أنواع الجرائم إبلاغًا إلى IC3 التابع لـ FBI في عام 2025، بواقع 191,561 شكوى. [2]

2. نظرة على الأمن

تسبب اختراق البريد الإلكتروني للأعمال (BEC) في خسائر تزيد على 3 مليارات دولار أُبلغ عنها إلى IC3 التابع لمكتب FBI في عام 2025. [2]

3. نظرة على الأمن

تختلف النطاقات المنتحلة بالأخطاء المطبعية عن أسماء العلامات التجارية الحقيقية بحرف أو حرفين، لذا قد تفوتك بنظرة سريعة.

4. نظرة على الأمن

تسببت عمليات احتيال الدعم الفني في خسائر تتجاوز 2.1 مليار دولار أُبلغ عنها إلى IC3 التابع لمكتب FBI في 2025. [2]

5. نظرة على الأمن

تبدو هجمات التماثل الحرفي (Homograph) متطابقة في شريط عنوان المتصفح ما لم يعرض المتصفح إعدادات punycode.

6. نظرة على الأمن

تستخدم الاحتيالات عبر الرسائل النصية (smishing) رسائل قصيرة عاجلة تتضمن روابط، مما يترك للضحايا سياقًا ضئيلًا لاكتشاف الاحتيال.

7. رؤية حول الأمان

تستهدف هجمات صيد الحيتان بريد المديرين التنفيذيين لأنهم يتحكمون في الوصول إلى حوالات الدفع الكبيرة.

8. رؤية حول الأمان

يُعد التحقق من تغييرات الدفع بالاتصال برقم هاتف معروف ومحفوظ دفاعًا رئيسيًا ضد احتيال التحويلات BEC.

9. رؤية حول الأمان

مواقع الضمان المزيفة عملية احتيال شائعة في الأسواق الإلكترونية: تبدو كخدمة دفع آمنة لكنها تسرق حوالة المشتري المصرفية.

10. نظرة على الأمن

ينبّه Google Safe Browsing المستخدمين قبل فتح المواقع التي وسمها بالتصيّد الاحتيالي أو البرمجيات الخبيثة.

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.). 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

مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

1 **السؤال 1** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما المؤشر الرئيسي على احتيال الدعم الفني؟ → نافذة منبثقة تدّعي أن نظامك مصاب وتطالبك بالاتصال برقم هاتف

2 **السؤال 2** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الأسلوب الذي يستخدم نطاقات مرسل منتحلة لسرقة بيانات الحسابات المصرفية؟ → التصيّد الاحتيالي عبر البريد الإلكتروني

3 **السؤال 3** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ما الذي يمثل احتيال التحويل المصرفي؟ → خداع الضحايا لإرسال الأموال إلى حسابات شركات مزيفة باستخدام الهندسة الاجتماعية

4 **السؤال 4** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

لماذا ينشئ المحتالون مواقع تسوق مزيفة؟ → لسرقة تفاصيل بطاقات الائتمان وبيانات اعتماد الدفع من المشترين

5 **السؤال 5** — الإجابة الصحيحة: **A**

ملاحظة للمعلم

ماذا يعني التصيّد الصوتي (Vishing)؟ → عمليات احتيال التصيّد الصوتي عبر شبكات الهاتف لسرقة بيانات الاعتماد

مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

6 السؤال 6

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: يستهدف التصيّد الاحتيالي المديرين التنفيذيين أيضًا؛ والصيد الأكبر (whaling) تصيّد احتيالي موجه إلى كبار القادة.

7 السؤال 7

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تستخدم النطاقات المنتحلة غالبًا أخطاء إملائية طفيفة (مثل amaz0n.com) لمحاكاة العلامات التجارية الموثوقة.

8 السؤال 8

الإجابة الصحيحة: خطأ

ملاحظة للمعلم

خطأ: منح محتال الدعم الفني وصولًا عن بُعد يتيح له زرع برمجيات خبيثة وسرقة البيانات.

9 السؤال 9

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

تستغل الهندسة الاجتماعية علم النفس البشري مثل الخوف والاستعجال لتجاوز قواعد الأمان.

10 السؤال 10

الإجابة الصحيحة: صحيح

ملاحظة للمعلم

ينبغي دائمًا التحقق من طلبات التحويل المصرفي عبر قنوات اتصال خارج النطاق.

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

G 1. التصيّد الاحتيالي	F 2. منتحِل	D 3. التصيّد الصوتي	B 4. احتيال
H 5. التحقق	A 6. التحويل المصرفي	E 7. صيد الحيتان	C 8. التصيّد بالرسائل

نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

1 التصيد الاحتيالي	2 منتحلة	3 التصيد الصوتي	4 احتيال
5 التحقق	6 التحويل		

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

1 B – منتحلة	2 E – التحقق	3 F – التحويل	4 H – النصية
5 G – الحيتان	6 C – الصوتي	7 A – التصيد	8 D – الاحتيال

ملاحظات النقاش للمعلمين

المصطلحات الأساسية:
تحقّق من قدرة الطلاب على شرح التصيّد الاحتيالي ومنتحِل والتصيّد الصوتي 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	ك	ي	ز	د	ع	ك	ط	ق	و	ق	ع	ت	م	ل
ل	ح	ت	ش	س	ب	ا	ب	ا	ت	ف	ي	ش	س	ي
ش	و	و	م	ش	ج	ق	ط	س	ل	ج	ز	ط	ط	ش
ق	ف	س	ة	ل	ح	ت	ن	م	ر	ت	ط	ط	ق	ك
ل	م	ل	د	م	ا	ب	ل	ق	ق	ع	س	ز	ك	ب
ن	ه	ا	ج	ل	ل	ا	ة	ن	ق	ت	ة	ي	ه	د
ا	ش	ر	ة	ج	ا	ط	ج	ل	ك	ح	و	ف	د	ب
ت	ن	ب	ا	ة	ح	ع	ج	ش	ت	ا	ت	ج	ع	ج
ي	ح	ر	ز	ج	ت	ك	ق	ط	ح	ح	ز	ل	ك	ة
ح	ل	ح	ك	ه	ي	ا	ح	ا	ا	ك	و	ف	ا	ط
ل	ف	م	و	ق	ا	ل	س	ك	م	ل	ت	ي	ط	ي
ا	ب	و	ك	د	ل	و	ن	ل	س	ا	ة	ي	ل	ي
س	د	ز	ط	ك	س	س	س	م	ف	ر	ق	ق	ر	ر
ة	ا	ع	ن	د	ن	ي	ب	ي	ك	ي	ب	ر	س	ة
د	س	ع	ف	ع	و	ة	ت	س	ة	ي	د	ي	ف	ه

حل الكلمات المتقاطعة

			ل	ا	ي	ت	ح	ا	ل	ا
ا		م		ل				ل		ل
ل		ن		ت				ت		ت
ن	ا	ت	ي	ح	ل	ا		ص		ح
ص		ح		و		ل		ي		ق
ي		ل		ي		ص		د		ق
ة		ة		ل		و				
						ت				
						ي				

دليل المعلم لحلول الكلمات المتقاطعة

أفقي

1 أفقي: الاحتيال مخطط خادع يهدف إلى سرقة المال أو بيانات الدخول من الضحايا (8 حروف)

6 أفقي: الحيتان هجمات تصيد موجهة تستهدف سرقة بيانات الدخول من كبار المديرين التنفيذيين (7 حروف)

عمودي

1 عمودي: التحقق تأكيد تفاصيل الدفع عبر وسيلة تواصل ثانوية موثوقة (6 حروف)

2 عمودي: التصيد حملات بريد احتيالية مصممة لسرقة بيانات الدخول وكلمات المرور (6 حروف)

3 عمودي: التحويل إعادة توجيه خادعة للمعاملات المصرفية إلى حسابات المجرمين (7 حروف)

4 عمودي: منتحلة عنوان مرسل أو موقع محاكى مصمم ليبدو مشروعا (6 حروف)

5 عمودي: النصية إرسال رسائل نصية احتيالية لسرقة بيانات دخول حسابات الجوال (6 حروف)

6 عمودي: الصوتي مكالمات صوتية احتيالية مصممة لسرقة بيانات الدخول وتفاصيل الحسابات (6 حروف)

مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

مفتاح ترتيب الكلمات المبعثرة

1. تاصيدل — التصيد
2. ياصتول — الصوتي
3. اتحققل — التحقق
4. نلتياح — الحيتان
5. حتةملن — منتحلة
6. الحياتلا — الاحتيال
7. ايوللحت — التحويل
8. نةايصل — النصية

مفتاح تحدي الشيفرة السرية

"اكتشف حملات التصيد بالتحقق عبر ماسح"

مفتاح إجابات دراسات الحالة

A دراسة الحالة 1: منع احتيال التحويلات البنكية في الشركات

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: يتلقى قسم المالية رسالة بريد إلكتروني عاجلة من عنوان مورد منتحَل، تطلب توجيه تحويلات الفواتير المستقبلية إلى رقم توجيه جديد.
- الاستراتيجية والحل الموصى بهما: فرض سياسة التفويض المزدوج لجميع المدفوعات. تنفيذ التحقق خارج النطاق باستخدام رقم هاتف محفوظ مسبقًا، وحظر رسائل البريد المنتحلة للنطاق عند البوابة.

B دراسة الحالة 2: حادثة تصيّد احتيالي لصيد الحيتان على التنفيذيين

حل المعلم

دليل التصحيح

ينبغي أن تغطي إجابات الطلاب النقاط التالية:

- تحليل السيناريو: نقر أحد المديرين التنفيذيين على رابط تصيّد احتيالي يزعم أنه يحتوي على وثيقة آمنة لاجتماع مجلس الإدارة، وأدخل بيانات اعتماده المؤسسية الرئيسية في بوابة مزيفة.
- الاستراتيجية والحل الموصى بهما: اعزل جهاز المدير التنفيذي. وأعد تعيين جميع رموز الجلسات وبيانات الاعتماد في الشركة. راجع سجلات الوصول بحثًا عن تسرب البيانات، وطبّق المصادقة متعددة العوامل بالعتاد على جميع عمليات تسجيل الدخول.