الاسم: _____ التاريخ: _____ الدرجة: _____

# هجمات التصيّد الاحتيالي والهندسة الاجتماعية

التصيّد الموجّه، وعمليات احتيال الصيد الكبير (whaling)، وبروتوكولات SPF/DKIM/DMARC، وانتحال المرسل، وتدريب الموظفين على الأمان.

## نظرة عامة على التعلّم: هجمات التصيّد الاحتيالي

**مرحبًا!** ترشدك حزمة الأنشطة هذه عبر التصيّد الاحتيالي والهندسة الاجتماعية. ستستكشف التصيّد الموجّه وصيد الحيتان وانتحال النطاقات وبروتوكولات SPF/DKIM/DMARC وأمان الروابط والتدريب على التوعية للموظفين.

**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/phishing-attacks/

# خارطة طريقك لتعلّم الحد من التصيّد الاحتيالي

- تعرّف على عمليات التصيّد الاحتيالي والتصيّد الصوتي والنوافذ المنبثقة الشائعة لاحتيال الدعم الفني.
- طبّق إجراءات التحقق من المعاملات عبر قناة خارجية.
- هيّئ قواعد SPF وDKIM وDMARC لحظر النطاقات المنتحلة.

### تعليمات دليل هجمات التصيّد الاحتيالي

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 مصادقة البريد الإلكتروني. واختم بالنشاط الإضافي «فكّر بسرعة».

### هجمات التصيّد الاحتيالي والهندسة الاجتماعية (مقدمة)

تستخدم هجمات التصيّد الاحتيالي رسائل موجهة وعمليات احتيال الحيتان وانتحال النطاقات لجمع بيانات تسجيل دخول المستخدمين. ويتطلب تأمين أنظمة الشركات نشر قواعد SPF وDKIM وDMARC عند البوابة إلى جانب خطوات موافقة عبر قناة منفصلة.

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

## نقطة التحقق 1: تحدي الاختيار من متعدد

**1. ما هو التصيّد الموجّه؟**

- A. رسالة تصيّد احتيالي موجّهة مصممة لفرد أو مؤسسة بعينها
- B. رسالة بريد جماعية واسعة تُرسل إلى ملايين العناوين العشوائية
- C. هجوم شبكي يغمر خوادم الويب بحركة المرور
- D. أسلوب استخراج قواعد بيانات يستهدف سجلات المستخدمين

**2. أي بروتوكول يتيح لنطاق إدراج عناوين IP المرسلة المصرح بها في DNS لمكافحة الانتحال؟**

- A. SPF
- B. DKIM
- C. DMARC
- D. HTTPS

**3. ما هو هجوم صيد الحيتان؟**

- A. حملة تصيّد احتيالي موجّهة تحديدًا إلى كبار التنفيذيين في الشركات المعروفين
- B. هجوم حقن SQL يستهدف النسخ الاحتياطية لقواعد البيانات
- C. سرقة مادية لمعدات موجّه الشبكة المحلية
- D. فحص آلي بالقوة الغاشمة لحشو بيانات الاعتماد

**4. ماذا يفعل DKIM؟**

- A. يضيف توقيعًا تشفيريًا إلى الرسائل الإلكترونية للتحقق من صحة هوية المرسل
- B. يحظر حركة حزم الشبكة الواردة عند جدار الحماية
- C. يشفّر وحدات تخزين قواعد البيانات أثناء السكون
- D. يفحص مرفقات البريد الإلكتروني بحثًا عن البرمجيات الخبيثة المعتمدة على التوقيعات

**5. ما دور DMARC؟**

- A. توجيه خوادم البريد المستقبِلة بكيفية التعامل مع فحوص SPF/DKIM الفاشلة
- B. فك تشفير كلمات مرور النظام باستخدام جداول قوس قزح محسوبة مسبقًا
- C. ضغط مرفقات البريد الإلكتروني قبل التسليم
- D. تهيئة صلاحيات الوصول إلى توجيه الشبكة

## نقطة التحقق 2: تحدي صحيح أم خطأ

**6 سؤال 6**

6. يعتمد التصيّد الموجّه على رسائل بريد إلكتروني جماعية عامة تُرسل إلى ملايين العناوين العشوائية.

صحيح ○ خطأ ○

**7 سؤال 7**

7. يمكن لسياسات DMARC أن توجّه خوادم البريد إلى رفض الرسائل المنتحلة غير المصرّح بها.

صحيح ○ خطأ ○

**8 سؤال 8**

8. يعمل التحقق من SPF بالتحقق من التوقيع التشفيري لنص رسالة البريد الإلكتروني.

صحيح ○ خطأ ○

**9 سؤال 9**

9. تستهدف هجمات صيد الحيتان مسؤولي الشركات من المستوى الأدنى للوصول إلى ملفات قواعد البيانات.

صحيح ○ خطأ ○

**10 سؤال 10**

10. يساعد التحقق خارج النطاق من طلبات الدفع في إيقاف عمليات احتيال التحويلات المصرفية.

صحيح ○ خطأ ○

## نقطة التحقق 3: إدراج المصطلحات الأساسية

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

1. يسمى استهداف موظف بعينه بمعلومات شخصية التصيد الاحتيالي _____ .
2. تزوير ترويسة البريد لجعل الرسائل تبدو مشروعة هو _____ المرسل.
3. قائمة سجلات DNS لعناوين IP لخوادم البريد المصرح بها هي _____ .
4. معيار توقيع البريد الذي يوفر التحقق من المرسل هو _____ .
5. يعتمد وضع سياسات لرفض فحوص SPF وDKIM الفاشلة على _____ .
6. تسمى حملة التصيد التي تستهدف كبار المديرين التنفيذيين صيد _____ .

بنك كلمات المفردات

التوقيع | الحيتان | المرسلين | الموجه | انتحال | DKIM | DMARC | SPF

اكتب إجاباتك هنا:

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

# نقطة التحقق 4: مطابقة مفاهيم الأمان

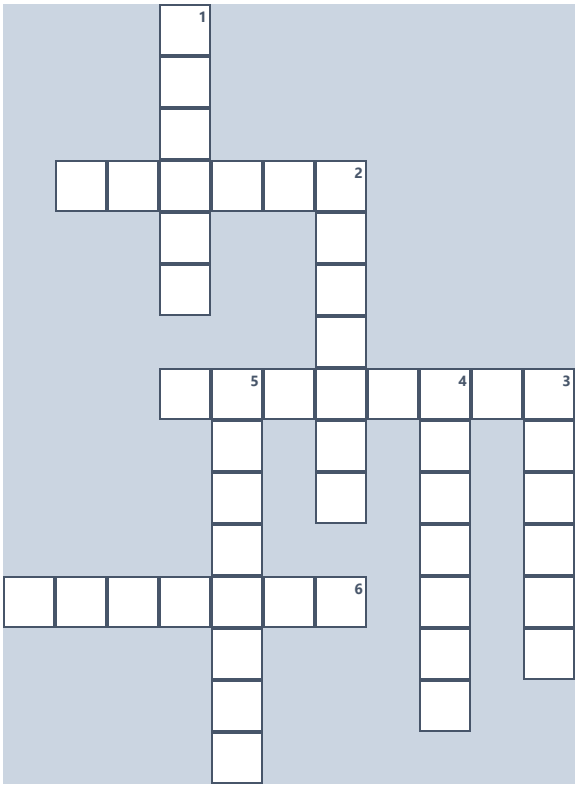
### مطابقة التعريفات

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

| | | | |
|---|---|---|---|
| 1. الموجَّه | | A | مكالمات احتيال صوتية. |
| 2. الانتحال | | B | استهداف المديرين التنفيذيين من الإدارة العليا. |
| 3. SPF | | C | تعليمات رفض السياسة. |
| 4. DKIM | | D | عناوين IP للمُرسِلين المصرّح لهم في DNS. |
| 5. DMARC | | E | بريد إلكتروني للهندسة الاجتماعية. |
| 6. صيد الحيتان | | F | بريد إلكتروني مخصص موجّه. |
| 7. التصيّد الاحتيالي | | G | انتحال عنوان البريد الإلكتروني للمرسل. |
| 8. التصيّد الصوتي | | H | توقيع تشفيري في البريد الإلكتروني. |

## نقطة التحقق 5: لغز الكلمات المتقاطعة

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




### أفقي

**2. بريد إلكتروني مخصص يستهدف شخصا بعينه (6)**

**3. تزوير عنوان البريد الإلكتروني للمرسل (8)**

**6. تعليمات رفض الرسائل التي تفشل في الفحص (7)**

### عمودي

**1. مكالمات احتيالية تعتمد على الصوت (6)**

**2. استهداف كبار المديرين التنفيذيين (7)**

**3. بريد إلكتروني قائم على الهندسة الاجتماعية (6)**

**4. توقيع تشفيري مضمن في البريد الإلكتروني (7)**

**5. عناوين IP المصرح لها بإرسال البريد المسجلة في DNS (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: بريد إلكتروني مخصص يستهدف شخصا بعينه (6 حروف):**

**3 أفقي: تزوير عنوان البريد الإلكتروني للمرسل (8 حروف):**

**6 أفقي: تعليمات رفض الرسائل التي تفشل في الفحص (7 حروف):**

### عمودي

**1 عمودي: مكالمات احتيالية تعتمد على الصوت (6 حروف):**

**2 عمودي: استهداف كبار المديرين التنفيذيين (7 حروف):**

**3 عمودي: بريد إلكتروني قائم على الهندسة الاجتماعية (6 حروف):**

**4 عمودي: توقيع تشفيري مضمن في البريد الإلكتروني (7 حروف):**

**5 عمودي: عناوين IP المصرح لها بإرسال البريد المسجلة في DNS (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 | ك | ه | ز | د | ع | ك | ا | ط | ق | و | ق | ع | ت | م |
| ل | ل | ج | ح | ش | س | ب | ل | ا | ا | ب | ت | ف | ي | ش |
| س | ي | و | ش | و | م | ش | ح | ج | ل | ق | ط | س | ج | ز |
| ط | ط | م | ش | ق | ف | ر | ي | ط | س | ق | ك | ل | م | |
| م | د | ل | ب | ل | ا | ق | ت | د | ع | ز | ي | ك | ب | ه |
| ع | ج | ا | ل | ة | ل | ن | ا | ت | ي | ة | ه | ا | د | ش |
| ي | ر | ة | ج | ط | ا | ج | ن | ل | ك | ص | و | ف | س | ب |
| ق | ن | ب | ا | ة | ن | ع | ج | ش | م | ا | ت | ج | ع | ة |
| و | ج | ح | ر | ز | ت | ج | ك | ق | ط | ر | ح | ل | ز | ك |
| ت | ة | ل | ح | ك | ح | ا | ه | ح | ا | ا | س | ك | ا | ف |
| ل | ط | ف | م | و | ا | ل | ق | س | ك | م | ل | ل | ت | ط |
| ا | ي | ب | د | ك | ل | ص | و | و | س | ا | ك | ة | ي | ي |
| ي | ص | د | ز | ط | ك | و | س | ص | ص | م | ف | ر | ق | ن |
| ق | ر | ة | ا | ع | ن | ت | د | ن | ب | ي | ك | ي | ب | ر |
| ص | ة | د | س | ع | ف | ي | ع | و | ت | ص | ة | ي | د | ي |

### قائمة كلمات المفردات

الموجه | الانتحال | المرسلين | التوقيع | السياسة | الحيتان | التصيد | الصوتي

## 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.** الموجه |
| **B.** الانتحال |
| **C.** المرسلين |
| **D.** التوقيع |
| **E.** السياسة |
| **F.** الحيتان |
| **G.** التصيد |
| **H.** الصوتي |

| التعريفات وحقول المطابقة |
| --- |
| 1. تزوير عنوان البريد الإلكتروني للمرسل. |
| 2. بريد إلكتروني مخصص يستهدف شخصا بعينه. |
| 3. مكالمات احتيالية تعتمد على الصوت. |
| 4. عناوين IP المصرح لها بإرسال البريد المسجلة في DNS. |
| 5. بريد إلكتروني قائم على الهندسة الاجتماعية. |
| 6. تعليمات رفض الرسائل التي تفشل في الفحص. |
| 7. توقيع تشفيري مضمن في البريد الإلكتروني. |
| 8. استهداف كبار المديرين التنفيذيين. |

## 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. م ا و ج ه ل
2. ر ا ن ل ي ل س م
3. ي ا ا ة س س ل
4. د ص ت ي ا ل
5. ت ح ل ل ن ا ا
6. ي ت ق ا و ع ل
7. ا ا ت ن ل ي ح
8. ص ي ا ت و ل

# نشاط إضافي: فكّر بسرعة

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

| | | | |
|---|---|---|---|
| 1 | أجهزة يمكن اختراقها | | | |
| 2 | علامات رسالة التصيّد الاحتيالي | | | |
| 3 | علامات إصابة الحاسوب | | | |
| 4 | كلمات تخلق إحساسًا زائفًا بالاستعجال | | | |
| 5 | طرق للتحقق من المرسل | | | |
| 6 | أشخاص يمكنك طلب مساعدة تقنية منهم | | | |
| 7 | أشياء تحتفظ بنسخة احتياطية منها | | | |
| 8 | أسماك أو كائنات بحرية تعرفها | | | |
| 9 | شركات ينتحل المحتالون صفتها | | | |
| 10 | عادات آمنة يمكنك البدء بها اليوم | | | |
| 11 | أشياء تفعلها بعد النقر على رابط مزيف | | | |
| 12 | أشياء تفعلها بعد تسرّب البيانات | | | |
| 13 | قنوات يحدث فيها التصيّد الاحتيالي | | | |
| 14 | أشياء لا ترسلها أبدًا بالبريد الإلكتروني | | | |
| 15 | طرق لحماية حساباتك | | | |

# نقطة التحقق 8: دراسات حالة في الأمن السيبراني

طبّق المفاهيم التي تعلمتها لحل السيناريوهات الواقعية أدناه.

### دراسة الحالة 1: معالجة هجوم صيد الحيتان على كبار التنفيذيين



**السيناريو:** يتلقى المدير المالي بريدًا إلكترونيًا مخصصًا بدقة عالية يدّعي أنه من الرئيس التنفيذي، يطلب تحويلًا سريعًا بمبلغ 50,000 دولار لإتمام شراء نطاق سري.

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

### دراسة الحالة 2: نشر سياسات بوابة SPF/DKIM/DMARC



**السيناريو:** تفشل مؤسسة في عمليات التدقيق الأمني لأن رسائل التسويق الصادرة تُصنَّف كثيرًا على أنها بريد مزعج، ولأن المخترقين ينتحلون بنشاط نطاق علامة الشركة التجارية.

**سؤال للنقاش:** ضع ضوابط تقنية وإدارية للتحقق من أصالة البريد الإلكتروني.

## 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 | 12 | 8 | 25 | 26 | 23 | 1 | | 20 | 13 | 3 | 22 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |

| 21 | 28 | 21 | 8 | 3 | 2 | | 29 | 28 | 18 | 1 | 24 | 3 | 5 | 1 | 23 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | |

| 8 | 28 | 10 | 2 | 23 | 1 | | 29 | 2 | 1 | 27 | 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 التصيّد الاحتيالي؟**

التصيّد الاحتيالي هجوم هندسة اجتماعية يرسل فيه المجرمون رسائل احتيالية لخداع المستخدمين كي يشاركوا بيانات حساسة.

**Q2: ما الفرق بين التصيّد الاحتيالي والتصيّد الموجّه؟**

يستهدف التصيّد الاحتيالي مجموعات واسعة بمحتوى عام، بينما يستهدف التصيّد الموجّه ضحايا محددين باستخدام تفاصيل مخصصة.

**Q3: ما صيد الحيتان (whaling)؟**

صيد الحيتان هجوم تصيّد احتيالي موجّه بدقة يستهدف كبار التنفيذيين الذين يملكون صلاحيات إدارية.

**Q4: ما انتحال البريد الإلكتروني؟**

انتحال البريد الإلكتروني هو إنشاء رسائل بريد إلكتروني بعنوان مرسل مزوّر لخداع المستلم كي يثق بالمصدر.

**Q5: كيف يمنع SPF الانتحال؟**

ينشر قائمة بعناوين IP المصرّح لها بالإرسال في DNS، ما يتيح للخوادم المستقبِلة التحقق من مصدر البريد. [1]

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

راجع الأسئلة والأجوبة الشائعة حول الحد من التهديدات عبر الإنترنت.

### Q6: ما DKIM؟

يضيف DomainKeys Identified Mail توقيعًا تشفيريًا إلى ترويسات البريد الإلكتروني، يثبت أن نطاقًا ما تحمّل المسؤولية وأن الرسالة لم تُعدَّل.

### Q7: ماذا تعني DMARC اختصارًا؟

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

### Q8: ما سياسة DMARC؟

سياسة تخبر خوادم البريد كيف تتعامل مع الرسائل التي تفشل في SPF/DKIM (لا شيء أو حجر أو رفض). [2]

### Q9: ما التصيّد الصوتي (vishing)؟

التصيّد الصوتي، حيث يستخدم المهاجمون مكالمات هاتفية احتيالية لانتزاع بيانات إدارية أو مالية.

### Q10: كيف تساعد أدوات فحص الروابط؟

تفحص روابط البريد الإلكتروني الواردة وتعيد كتابتها للتحقق من أمان صفحات الويب الوجهة وقت النقر.

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

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

**Q1: كيف يعمل هجوم التماثل الحرفي؟**

يسجّل المهاجمون أسماء نطاقات باستخدام أحرف Unicode غير ASCII مشابهة في الشكل لمحاكاة اسم نطاق مشروع بصريًا.

**Q2: ما تمثيل Punycode؟**

ترميز يحوّل أسماء النطاقات بصيغة Unicode إلى سلاسل متوافقة مع ASCII تبدأ بـ 'xn--' ليتمكن DNS من التعامل معها.

**Q3: لماذا تُعد حالة 'p=reject' الأكثر أمانًا في DMARC؟**

يطلب من الخوادم المستقبِلة رفض البريد الذي يفشل في DMARC (SPF/DKIM المتوافقين) أثناء جلسة SMTP، فيحجب الانتحال المباشر. [2]

**Q4: كيف يتجاوز المهاجمون قواعد SPF؟**

باستغلال نطاقات مشابهة في الشكل (typosquatting) أو باستخدام حسابات مخترقة على خدمات بريد خارجية مشروعة.

**Q5: ما اختراق البريد الإلكتروني للأعمال (BEC)؟**

عملية احتيال مؤسسية يختطف فيها المهاجمون حسابات البريد الإلكتروني للشركات أو ينتحلونها لاعتماد مدفوعات احتيالية.

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

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

### Q6: كيف توقف المصادقة متعددة العوامل التصيّد الاحتيالي؟

يتطلب رموزًا ثانوية (مثل مفاتيح الأجهزة) لا يمكن سرقتها عبر صفحات هبوط مقلّدة وحدها.

### Q7: ما صفحة الهبوط لحصاد بيانات الاعتماد؟

بوابة تسجيل دخول مزيفة مشابهة للأصل مصممة لالتقاط أسماء المستخدمين وكلمات المرور ورموز MFA المُدخلة في الوقت الفعلي.

### Q8: ما اختطاف النطاق الفرعي؟

مهاجم يسيطر على مؤشر نطاق فرعي DNS غير مستخدم لاستضافة صفحات هبوط تصيّد خبيثة تحت نطاق أصل موثوق.

### Q9: كيف يعمل فحص محاذاة DKIM؟

يتحقق من أن النطاق في ترويسة 'From' يطابق النطاق الذي وقّع الرسالة تشفيريًا في ترويسة DKIM.

### Q10: ما دور بوابة البريد الإلكتروني؟

تصفية البريد الإلكتروني الوارد، وتدقيق الروابط، وعزل المرفقات في بيئة معزولة، والتحقق من الامتثال لـ SPF/DKIM/DMARC.

# 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. [4]

**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. [4]

**3. نظرة على الأمن**

تستخدم هجمات التماثل الحرفي حروفًا سيريلية مشابهة لتكرار نطاقات العلامات التجارية المطابقة تمامًا بصريًا في المتصفحات.

**4. نظرة على الأمن**

مع 'p=reject'، يطلب النطاق من المستقبِلين رفض البريد الفاشل أثناء التسليم، لا وضعه في البريد غير المرغوب. [2]

**5. نظرة على الأمن**

كثيرًا ما تطلب هجمات صيد الحيتان التي تستهدف الرؤساء التنفيذيين دفعات عاجلة لصفقات اندماج سرية أو شراء نطاقات.

**6. نظرة على الأمن**

تنسخ بوابات حصاد بيانات الاعتماد صفحات تسجيل الدخول الحقيقية فيكتب الضحايا كلمات المرور مباشرةً في نموذج المهاجم.

**7. رؤية حول الأمان**

يوصي إرشاد CISA المشترك بشأن التصيّد الاحتيالي بتدريب المستخدمين إلى جانب DMARC وSPF وDKIM والمصادقة متعددة العوامل المقاومة للتصيّد. [3]

**8. رؤية حول الأمان**

يقتصر تقييم SPF على 10 مصطلحات تستعلم عن DNS؛ وتجاوز هذا الحد يعيد نتيجة 'permerror'. [1]

**9. رؤية حول الأمان**

توفر مفاتيح الأمان المادية FIDO2 حماية مدعومة تشفيريًا ضد حصاد بيانات الاعتماد عن بُعد.

**10. نظرة على الأمن**

التصيّد الاحتيالي من أكثر الطرق شيوعًا التي يدخل بها المهاجمون إلى مؤسسة لأول مرة، ولهذا فإن التدريب المنتظم على التوعية دفاع فعّال.

# المراجع والمصادر التقنية

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

### المراجع الأكاديمية والصناعية

[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

## مفتاح الإجابة: نقطة التحقق 1 - اختيار من متعدد

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

**ملاحظة للمعلم**

ما هو التصيّد الموجّه؟ ← رسالة تصيّد احتيالي موجّهة مصممة لفرد أو مؤسسة بعينها

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

**ملاحظة للمعلم**

ينشر SPF مضيفي الإرسال المصرح بهم للنطاق في DNS حتى يتمكن المستقبلون من التحقق من مرسل المغلف.

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

**ملاحظة للمعلم**

ما هو هجوم صيد الحيتان؟ ← حملة تصيّد احتيالي موجّهة تحديدًا إلى كبار التنفيذيين في الشركات المعروفين

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

**ملاحظة للمعلم**

ماذا يفعل DKIM؟ ← يضيف توقيعًا تشفيريًا إلى الرسائل الإلكترونية للتحقق من صحة هوية المرسل

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

**ملاحظة للمعلم**

ما دور DMARC؟ ← توجيه خوادم البريد المستقبِلة بكيفية التعامل مع فحوص SPF/DKIM الفاشلة

## مفتاح الإجابة: نقطة التحقق 2 - صحيح أو خطأ

**6 السؤال 6**

الإجابة الصحيحة: خطأ

### ملاحظة للمعلم

خطأ: يُصمَّم التصيّد الاحتيالي الموجه لأشخاص محددين، بخلاف التصيّد الاحتيالي الجماعي العام.

**7 السؤال 7**

الإجابة الصحيحة: صحيح

### ملاحظة للمعلم

يمكن لسياسات DMARC أن توجّه خوادم البريد إلى رفض الرسائل المنتحلة غير المصرّح بها.

**8 السؤال 8**

الإجابة الصحيحة: خطأ

### ملاحظة للمعلم

خطأ: يتحقق SPF من عنوان IP المرسل مقابل DNS؛ أما DKIM فهو الذي يتحقق من توقيع تشفيري.

**9 السؤال 9**

الإجابة الصحيحة: خطأ

### ملاحظة للمعلم

خطأ: يستهدف الصيد الأكبر (whaling) كبار المسؤولين التنفيذيين، الذين يمكنهم الموافقة على المدفوعات والوصول إلى بيانات حساسة.

**10 السؤال 10**

الإجابة الصحيحة: صحيح

### ملاحظة للمعلم

صحيح: تأكيد طلبات الدفع عبر قناة منفصلة معروفة يساعد في إيقاف الاحتيال بالتحويلات المصرفية.

# 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

| | | | |
|---|---|---|---|
| F 1. الموجّه | G 2. الانتحال | D 3. SPF | H 4. DKIM |
| C 5. DMARC | B 6. صيد الحيتان | E 7. التصيّد الاحتيالي | A 8. التصيّد الصوتي |

## نقطة التحقق 3: مفتاح الإجابة – المصطلحات الأساسية

| | | | |
|---|---|---|---|
| 1 الموجه | 2 انتحال | 3 SPF | 4 DKIM |
| 5 DMARC | 6 الحيتان | | |

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

| | | | |
|---|---|---|---|
| 1 B – الانتحال | 2 A – الموجه | 3 H – الصوتي | 4 C – المرسلين |
| 5 G – التصيد | 6 E – السياسة | 7 D – التوقيع | 8 F – الحيتان |

### ملاحظات النقاش للمعلمين

**المصطلحات الأساسية:**
تحقّق من قدرة الطلاب على شرح الموجّه والانتحال وSPF 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 | ه | ز | د | ع | ك | ا | ط | ق | و | ق | ع | ت | م |
| ل | ل | ج | ح | ش | س | ب | ل | ا | ا | ب | ت | ف | ي | ش |
| س | ي | و | ش | و | م | ش | ح | ج | ل | ق | ط | س | ج | ز |
| ط | ط | م | ش | ق | ف | ر | ي | ط | ط | س | ق | ك | ل | م |
| م | د | ل | ب | ل | ا | ق | ت | د | ع | ز | ي | ك | ب | ه |
| ع | ج | ا | ل | ة | ل | ن | ا | ي | ة | ه | ا | د | ش | |
| ي | ر | ة | ج | ط | ا | ج | ن | ل | ك | و | ف | س | ب | |
| ق | ن | ب | ا | ة | ن | ع | ج | ش | م | ا | ت | ع | ة | |
| و | ج | ح | ر | ز | ت | ج | ك | ق | ط | ر | ح | ل | ك | |
| ت | ة | ل | ح | ك | ح | ا | ه | ا | ا | س | ك | ا | ف | |
| ل | ط | ف | م | و | ا | ل | ق | س | م | ك | ل | ت | ط | |
| ا | ي | ب | د | ك | ل | س | و | و | س | ا | ك | ة | ي | |
| ي | س | د | ز | ط | ك | و | س | س | ص | م | ف | ر | ق | ن |
| ق | ر | ة | ا | ع | ن | د | ت | ب | ن | ي | ك | ي | ب | ر |
| س | ة | د | س | ع | ف | ي | ع | و | ت | ص | ة | ي | د | ي |

## حل الكلمات المتقاطعة




## دليل المعلم لحلول الكلمات المتقاطعة

### أفقي

**2 أفقي: الموجه** بريد إلكتروني مخصص يستهدف شخصا بعينه (6 حروف)

**3 أفقي: الانتحال** تزوير عنوان البريد الإلكتروني للمرسل (8 حروف)

**6 أفقي: السياسة** تعليمات رفض الرسائل التي تفشل في الفحص (7 حروف)

### عمودي

**1 عمودي: الصوتي** مكالمات احتيالية تعتمد على الصوت (6 حروف)

**2 عمودي: الحيتان** استهداف كبار المديرين التنفيذيين (7 حروف)

**3 عمودي: التصيد** بريد إلكتروني قائم على الهندسة الاجتماعية (6 حروف)

**4 عمودي: التوقيع** توقيع تشفيري مضمن في البريد الإلكتروني (7 حروف)

**5 عمودي: المرسلين** عناوين IP المصرح لها بإرسال البريد المسجلة في DNS (8 حروف)

# مفتاح حل الكلمات المبعثرة والشيفرة

مفتاح تصحيح لنشاط فك خلط مفردات المصطلحات وتحدي الشيفرة السرية.

### مفتاح ترتيب الكلمات المبعثرة

1. ماوجهل → **الموجه**
2. رانليلسم → **المرسلين**
3. ياةسسل → **السياسة**
4. دصتيال → **التصيد**
5. تحللناا → **الانتحال**
6. يتقاوعل → **التوقيع**
7. اتنليح → **الحيتان**
8. صياتول → **الصوتي**

### مفتاح تحدي الشيفرة السرية

**"اكتشف الهندسة الاجتماعية بتدقيق بوابة البريد"**

# مفتاح إجابات دراسات الحالة

## A دراسة الحالة 1: معالجة هجوم صيد الحيتان على كبار التنفيذيين

حل المعلم

### دليل التصحيح

**ينبغي أن تغطي إجابات الطلاب النقاط التالية:**

- تحليل السيناريو: يتلقى المدير المالي رسالة بريد إلكتروني مخصصة للغاية تزعم أنها من الرئيس التنفيذي، تطلب تحويلًا سريعًا بمبلغ 50,000 دولار لإتمام شراء نطاق سري.
- الاستراتيجية والحل الموصى بهما: اضبط DMARC بسياسة 'p=reject' لحظر نطاقات المرسلين المنتحلة. وأضف لافتات تحذير للمرسلين الخارجيين عند البوابة، واشترط تأكيدًا شفهيًا خارج النطاق لجميع المعاملات المالية.

## B دراسة الحالة 2: نشر سياسات بوابة SPF/DKIM/DMARC

حل المعلم

### دليل التصحيح

**ينبغي أن تغطي إجابات الطلاب النقاط التالية:**

- تحليل السيناريو: تفشل مؤسسة في عمليات التدقيق الأمني لأن رسائل البريد الإلكتروني التسويقية الصادرة كثيرًا ما تُصنَّف كرسائل مزعجة، ولأن المخترقين ينتحلون بنشاط نطاق العلامة التجارية للشركة.
- الاستراتيجية والحل الموصى بهما: انشر سجل TXT لـ SPF يوضح عناوين IP المرسلة المصرح بها. واضبط مفاتيح توقيع DKIM على خوادم البريد الصادر، وحلّل تقارير ملاحظات DMARC بصيغة XML الواردة لتحديد إساءة الاستخدام.