

تم تحميل هذا الملف من موقع المناهج الإماراتية



## أسئلة اختبار درس المواطنة الرقمية

موقع المناهج ← المناهج الإماراتية ← الصف الثاني عشر ← اجتماعيات ← الفصل الثاني ← اختبارات ← الملف

تاريخ إضافة الملف على موقع المناهج: 2025-02-23 11:54:31

ملفات اكتب للمعلم اكتب للطالب الاختبارات الكترونية | اختبارات | حلول | عروض بوربوينت | أوراق عمل  
منهج انجليزي | ملخصات وتقارير | مذكرات وبنوك | الامتحان النهائي للمدرس

المزيد من مادة  
اجتماعيات:

إعداد: عمر حسن

## التواصل الاجتماعي بحسب الصف الثاني عشر



صفحة المناهج  
الإماراتية على  
فيسبوك

الرياضيات

اللغة الانجليزية

اللغة العربية

التربية الاسلامية

المواد على تلغرام

## المزيد من الملفات بحسب الصف الثاني عشر والمادة اجتماعيات في الفصل الثاني

الهيكل الامتحاني الوزاري الجديد كافة المسارات

1

عرض بوربوينت درس القواعد الإلكترونية

2

عرض بوربوينت حل درس الرؤية الثانية محو الأمية الإلكترونية

3

عرض بوربوينت درس مشروع الحماية الإلكترونية

4

عرض بوربوينت الفصل التاسع قيام الإمبراطوريات

5



### السؤال الأول 1: اختبار اختيار من متعدد حول موضوعات محددة

#### دراسة حالة 1: الابتزاز الإلكتروني

**المقدمة:** انتشر في الآونة الأخيرة عبر منصات التواصل الاجتماعي حالات من الابتزاز الإلكتروني التي تؤثر بشكل كبير على حياة الأفراد. وفقاً لإحصائيات أظهرت أن 32% من الشباب في سن 16-24 قد تعرضوا لمحاولات ابتزاز إلكتروني، بينما 15% منهم أفادوا بأنهم تعرضوا للابتزاز بالفعل.

**الأسئلة:**

1. وفقاً للدراسة، ما هي النسبة المئوية للشباب الذين تعرضوا لمحاولات ابتزاز إلكتروني؟

- أ) 25 % (ب) 32 % (ج) 15 % (د) 45 %

2. ما هي الإجراءات التي يجب اتخاذها عند التعرض للابتزاز الإلكتروني؟

- أ) التفاعل مع الشخص المبتز  
○ ب) إبلاغ السلطات المختصة وترك الرسائل كدليل  
○ ج) نشر الصور على الإنترنت للرد عليه  
○ د) إخفاء المعلومات عن العائلة

#### دراسة حالة 2: التنمر الإلكتروني

**المقدمة:** في عام 2024، أظهرت دراسة أن حوالي 20% من الطلاب في المدارس الثانوية تعرضوا للتنمر الإلكتروني. يعتقد بعض الخبراء أن هذه الظاهرة قد تؤدي إلى مشكلات نفسية تؤثر على أداء الطلاب الأكاديمي.

3. كم تبلغ نسبة الطلاب الذين تعرضوا للتنمر الإلكتروني وفقاً للدراسة؟

- أ) 10 % (ب) 15 % (ج) 20 % (د) 25 %

4. ما هو التأثير الأكثر شيوعاً للتنمر الإلكتروني على الطلاب؟

- أ) زيادة الأداء الدراسي  
○ ب) انخفاض الصحة النفسية  
○ ج) زيادة القدرة على استخدام التكنولوجيا  
○ د) تزايد المهارات الاجتماعية

#### دراسة حالة 3: الفجوة الرقمية

**المقدمة:** تشير التقارير إلى أن هناك فجوة رقمية كبيرة بين المناطق الحضرية والريفية في استخدام الإنترنت. وفقاً لمؤسسة الإحصاءات الوطنية، 60% من سكان المناطق الحضرية يتمتعون بإمكانية الوصول إلى الإنترنت عالي السرعة، بينما تقل النسبة إلى 30% في المناطق الريفية.

5. ما هي النسبة المئوية لسكان المناطق الحضرية الذين يتمتعون بإمكانية الوصول إلى الإنترنت عالي السرعة؟

- أ) 50 % (ب) 60 % (ج) 70 % (د) 80 %

6. ما هي العواقب المحتملة للفجوة الرقمية على التعليم؟

- أ) تعزيز التعليم عن بُعد  
○ ب) عدم تكافؤ الفرص في الحصول على المعرفة  
○ ج) زيادة فرص التعلم الذاتي  
○ د) تقليل الفجوة بين الطلاب

#### دراسة حالة 4: الشراء المندفع

**المقدمة:** أظهرت دراسة أجرتها إحدى شركات الاستطلاع في 2023 أن 40% من الأشخاص الذين قاموا بشراء منتجات عبر الإنترنت يعترفون بأنهم اشتروا المنتجات بدافع الاندفاع دون تخطيط مسبق.

**الأسئلة:**

7. كم هي النسبة المئوية للأشخاص الذين قاموا بشراء المنتجات بشكل مندفع؟

- أ) 30 % (ب) 40 % (ج) 50 % (د) 60 %

8. كيف يمكن تقليل تأثير الشراء المندفع؟

- أ) استخدام أساليب التسويق الرقمي بشكل أكثر جذباً  
○ ب) تحديد ميزانية واضحة قبل الشراء  
○ ج) التسوق بشكل أسرع  
○ د) شراء المزيد من المنتجات

#### دراسة حالة 5: المواقع الموثوقة

**المقدمة:** وفقاً لدراسة أجرتها منظمة حماية البيانات، فإن 70% من المستخدمين لا يميزون بين المواقع الموثوقة والمواقع المخادعة على الإنترنت، مما يعرضهم لخطر الاحتيال.

**الأسئلة:**

9. كم هي النسبة المئوية للمستخدمين الذين لا يستطيعون التمييز بين المواقع الموثوقة وغير الموثوقة؟

- أ) 60 % (ب) 70 % (ج) 80 % (د) 90 %

10. ما هو أفضل إجراء لضمان تصفح آمن على الإنترنت؟

- أ) استخدام برامج الحماية فقط  
○ ب) تأكيد الموقع من خلال الرابط وآراء المستخدمين  
○ ج) تجاهل أي تحذيرات تظهر أثناء التصفح  
○ د) استخدام شبكة الإنترنت العامة فقط

السؤال الثاني : بعد قراءة الشكل التالي أجب عن الأسئلة التالية ؟

**7 تعديلات على قانون مكافحة الشائعات والجرائم الإلكترونية بالإمارات**

**يناير 2020**  
بدء التنفيذ

**أهداف القانون**

- حماية المجتمع والمواقع والبيانات الحكومية
- حماية خصوصية الأشخاص
- مكافحة الشائعات وجرائم النصب والاحتيال

**7 تعديلات**

- يعاقب على جرائم التسول الإلكتروني
- يجرم اختراق المواقع والشبكات والنظم الإلكترونية بقصد الحصول على بيانات
- يجرم تداول شائعات من شأنها إلحاق ضرر بالمصلحة العامة
- يعاقب على جرائم النصب والاحتيال باستخدام وسائل تقنية
- يمنح الأدلة الإلكترونية حجية الأدلة الجنائية المادية في الإثبات الجنائي
- يقول التصالح مع المتهم في بعض الجرائم الإلكترونية
- منح الأدلة المستخرجة من برامج الحاسب حجية الأدلة الجنائية

**1- الفهم والاستيعاب**

- ما الهدف الأساسي من التعديلات على قانون مكافحة الشائعات والجرائم الإلكترونية؟
- (A) تعزيز العقوبات في الجرائم التقليدية  
(B) حماية المجتمع والبيانات الشخصية من الجرائم الإلكترونية  
(C) تقليل استخدام الإنترنت في الدولة  
(D) دعم الاقتصاد الوطني من خلال الجرائم الإلكترونية

**2- التحليل**

- ما الذي يمكن أن يكون السبب الرئيسي وراء تجريم اختراق المواقع الإلكترونية والشبكات؟
- (A) حماية حقوق الملكية الفكرية فقط  
(B) الحفاظ على الخصوصية ومنع سرقة المعلومات  
(C) تعزيز استخدام الإنترنت من قبل الأفراد  
(D) الحد من انتشار الشائعات

**3- التفكير النقدي**

- وفقاً للتعديلات المذكورة، ما الأثر المتوقع لتجريم نشر الشائعات على وسائل التواصل الاجتماعي؟
- (A) زيادة الشائعات بسبب العقوبات  
(B) تعزيز الثقة بين أفراد المجتمع  
(C) تقليل استخدام وسائل التواصل الاجتماعي  
(D) القضاء الكامل على الجرائم الإلكترونية

**4- التطبيق**

- إذا تم رصد شخص ينشر معلومات مضللة عن طريق وسائل التواصل الاجتماعي، ما الإجراء القانوني المتوقع وفقاً للتعديلات؟
- (A) غرامة مالية فقط  
(B) السجن أو الغرامة حسب خطورة الجريمة  
(C) الإغلاق الفوري لحساباته الإلكترونية  
(D) تحذيره شفهيًا في البداية



## تحصين الخصوصية ورصد الجرائم

منذ 2008 وإدارة المباحث الجنائية في شرطة دبي تعمل جاهدة لرصد وتقصي الجرائم الإلكترونية التي باتت مصدر مضايقة تصل إلى حد التهديد إلى الأشخاص والشركات من خلال اختراق المواقع الإلكترونية ناهيك عن الابتزاز والاحتيال الذي بات مُطاً يتخذه المجرمون سبيلاً لقضاء مآربهم الخبيثة. وفي المقابل دعاوى إلى تحصين البيانات الشخصية للحيلولة دون وقوع اختراقات للخصوصية تتخذ أوجهاً كثيرة على شاكلة الابتزاز والتهديد.

الحذر من رسائل  
الاصطياد التي ترد  
عبر الهاتف المتحرك



تجنّب استخدام  
كلمات السر  
الأكثر شيوعاً

عدم استخدام  
كلمة المرور ذاتها  
لكافة الحسابات

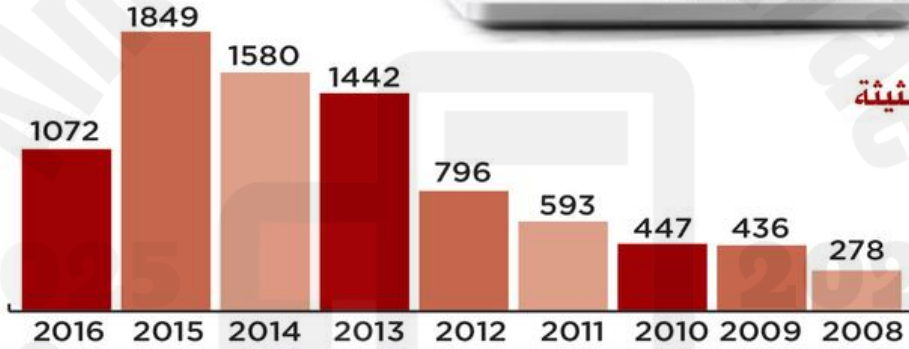


تجنّب استخدام  
شبكات الانترنت  
اللاسلكية العامة

تجنب فتح أي رسالة بريد  
إلكتروني قبل التأكد من  
مصدرها



آليات تحصينية



متابعة حثيثة

البيانات

غرافيك: حسام الحوراني

السؤال الثالث : بعد قراءة الشكل التالي أجب عن الأسئلة ؟

### 1- التحليل

ما السبب الذي أدى إلى انخفاض عدد الجرائم الإلكترونية بين عامي 2015 و2016؟

- A) زيادة العقوبات المفروضة على الجرائم الإلكترونية
- B) استخدام تقنيات متقدمة لرصد الجرائم وتعزيز الخصوصية
- C) تراجع استخدام الإنترنت في الدولة
- D) ضعف الأنظمة الأمنية في عام 2015

### 2- الفهم والتقييم

ما الهدف الأساسي من "آليات تحصينية" المذكورة في الصورة؟

- A) تقليل الرسائل الإلكترونية الواردة للمستخدمين
- B) منع حدوث الجرائم الإلكترونية عن طريق تعزيز سلوك الأمان الرقمي
- C) تحسين جودة خدمات الإنترنت العامة
- D) تسهيل استخدام كلمات المرور البسيطة

**3- التطبيق**

- أي من الخطوات التالية يجب أن يتبعها المستخدم عند استلام رسالة بريد إلكتروني غير معروفة المصدر؟
- A) فتح الرسالة للتأكد من محتواها  
B) حذف الرسالة فوراً لتجنب أي تهديد محتمل  
C) الرد على المرسل لتحديد الغرض من الرسالة  
D) مشاركة الرسالة مع الآخرين للتأكد من أنها آمنة

**4- التفكير النقدي**

- كيف يمكن أن يؤثر تجنب استخدام شبكات الإنترنت اللاسلكية العامة على حماية الخصوصية؟
- A) يمنع الوصول إلى المعلومات الشخصية من قبل المتسللين  
B) يقلل من سرعة الاتصال بالإنترنت  
C) يجعل المستخدمين غير قادرين على استخدام الإنترنت في الأماكن العامة  
D) يزيد من عدد الجرائم الإلكترونية في الشبكات العامة

**5- التحليل والاستنتاج**

- ما العلاقة بين زيادة عدد الجرائم الإلكترونية في عام 2013 وترجعها في السنوات اللاحقة؟
- A) تجاهل المستخدمين لقواعد الأمان في عام 2013  
B) تعزيز تقنيات الرصد والتحصين بعد عام 2013  
C) انخفاض استخدام الإنترنت بين عامي 2013 و2016  
D) ضعف النظام القانوني قبل عام 2013

**6- الفهم والتطبيق**

- ما الخطوة التي يجب اتخاذها لتجنب اختراق الحسابات وفقاً للآليات التحصينية؟
- A) استخدام كلمة مرور موحدة لجميع الحسابات  
B) تغيير كلمات المرور دورياً وعدم تكرارها  
C) عدم استخدام كلمات مرور معقدة لتسهيل التذكر  
D) استخدام نفس كلمة المرور لفترات طويلة

**7- التفكير النقدي والتقييم**

- كيف يمكن تقييم تأثير جهود شرطة دبي في رصد الجرائم الإلكترونية منذ عام 2008؟
- A) ارتفاع مستمر في عدد الجرائم حتى عام 2016  
B) انخفاض تدريجي في الجرائم الإلكترونية نتيجة جهود مكثفة  
C) عدم تأثير جهود الشرطة على معدلات الجرائم  
D) زيادة الجرائم بشكل ملحوظ منذ بدء التتبع

**8- التحليل والتطبيق**

- لماذا يُنصح بتجنب استخدام الأجهزة والوسائل العامة للاتصال عند التعامل مع معلومات حساسة؟
- A) لأنها تستهلك وقتاً أطول في التصفح  
B) لأنها تزيد من احتمالية تعرض البيانات للاختراق  
C) لأنها تتطلب برامج إضافية لتشغيلها  
D) لأنها تقلل من سرعة الشبكة

**9- التقييم**

- أي من الخيارات يعكس دور كلمات المرور المعقدة في تعزيز الأمن الإلكتروني؟
- A) تسهيل الوصول إلى الحسابات الشخصية  
B) زيادة صعوبة الاختراق وتقليل فرص الجرائم  
C) زيادة عبء المستخدم في تذكر كلمات المرور  
D) الحد من استخدام الحسابات الإلكترونية بشكل عام



### السؤال الرابع ؛ بعد قراءة النص قراءة متمنعة أجب عن الأسئلة التالية ؟

#### الفقرة:

تُعد الجرائم الإلكترونية من أخطر التحديات التي تواجه المجتمعات الحديثة، وقد تبنت الإمارات العربية المتحدة خطوات رائدة في التصدي لهذه الجرائم من خلال تطوير قوانين متقدمة. في عام 2020، تم إجراء تعديلات مهمة على قانون مكافحة الجرائم الإلكترونية، بهدف تعزيز حماية الأفراد والمؤسسات من الاختراقات والابتزاز الإلكتروني. يُجرّم القانون اختراق المواقع والشبكات الإلكترونية، والتلاعب بالبيانات، وانتحال الهوية الرقمية، كما يعاقب على نشر الشائعات والمعلومات المضللة التي تهدد السلم المجتمعي. ومن أبرز أهداف القانون تعزيز الأمن السيبراني، حماية الخصوصية، والحد من السلوكيات التي قد تؤدي إلى الإضرار بالمجتمع الرقمي. بالإضافة إلى ذلك، فرض القانون عقوبات صارمة تتراوح بين الغرامات المالية والسجن لضمان الردع الفعال. حرصت الجهات المختصة في الإمارات على تنفيذ هذا القانون بشكل صارم، حيث تمت ملاحقة المجرمين باستخدام أحدث التقنيات في التحليل والرصد. هذه الجهود تؤكد التزام الدولة بتحقيق بيئة رقمية آمنة ومستدامة.

#### أسئلة اختيار من متعدد:

##### 1- التحليل

ما الهدف الأساسي من تعديل قانون الجرائم الإلكترونية في الإمارات عام 2020؟

- A) تعزيز استخدام الإنترنت في المؤسسات الحكومية
- B) تقليل عدد المستخدمين للإنترنت في الدولة
- C) تعزيز الأمن السيبراني وحماية الأفراد من الابتزاز الرقمي
- D) تسهيل الوصول إلى بيانات المستخدمين

##### 2- الفهم والتقييم

وفقاً للقانون، ما العقوبة المحتملة لمن ينشر شائعات تضر بالسلم المجتمعي؟

- A) التحذير فقط
- B) الغرامة المالية والسجن
- C) تعليق الحساب الإلكتروني
- D) منعه من استخدام الإنترنت لمدة شهر

##### 3- التفكير النقدي

كيف يمكن أن يؤثر استخدام التقنيات المتقدمة في ملاحقة الجرائم الإلكترونية؟

- A) يزيد من صعوبة التعرف على المجرمين
- B) يساهم في تسريع عملية كشف الجناة ومحاسبتهم
- C) يقلل من استخدام الإنترنت بشكل عام
- D) يجعل التحقيقات أقل دقة

##### 4- التطبيق

إذا تلقت رسالة إلكترونية مشبوهة تطلب منك معلومات شخصية، فما التصرف الصحيح وفقاً لقانون الجرائم الإلكترونية؟

- A) تجاهل الرسالة وعدم الرد عليها
- B) تقديم المعلومات المطلوبة بسرعة
- C) مشاركة الرسالة مع الأصدقاء لتأكيد سلامتها
- D) حذف الرسالة بعد الرد عليها