حلول ملخص الاختبار الأول لمادة المهارات الرقمية للصف التاسع:

أشكال البيانات:

١. كمية
٢. نوعية
٣. مجردة

سبب ظهور أمن المعلومات:

- **أهمية المعلومات في اتخاذ القرارات.**

أمن المعلومات:

- **مجموعة من الاجراءات والتدابير الأمنية التي تشمل السياسات والاجراءات والتقنيات التي تحمي المعلومات الحساسة من سوء الاستخدام أو الوصول غير المصرح به أو التعطيل أو الاتلاف.**

أهمية أمن البيانات:

١. الحفاظ على الخصوصية: حماية البيانات الشخصية والحساسة من الوصول غير المصرح.
٢. ضمان التوافر: ضمان أن المعلومات متاحة عند الحاجة إليها.
٣. الامتثال للقوانين: من الأمثلة على تشريعات تلزم المؤسسات بحماية بيانات العملاء:
  - **CCPA**
  - **GDPR**

ملاحظات هامة:

١. أمن المعلومات يشمل الأمن السيبراني.
٢. الأمن السيبراني أوسع مجال من أمن المعلومات.

الأمن السيبراني:

- **هو الحماية والوقاية من الأخطار والتهديدات الموجودة في الفضاء الالكتروني أو الفضاء السيبراني الذي يشمل الإنترنت والشبكات الرقمية.**

العناصر الرئيسية لسياسة أمن المعلومات والأمن السيبراني:

١. أمن التطبيقات: النهج والإجراءات والأدوات وأفضل الممارسات التي توضع لحماية التطبيقات وبياناتها.
٢. التعافي من الكارثة: طريقة لإعادة إنشاء أنظمة تكنولوجية فعالة في أعقاب حدث والنسخ الاحتياطي المنتظم للبيانات.
٣. أمن البنية التحتية: الأمان الذي يشمل البنية التحتية التكنولوجية (الأجهزة الرقمية والبرامج).

ركائز أمن المعلومات:

١. السرية
٢. التوافر
٣. النزاهة

أفضل الممارسات لاستخدام كلمة السر لحماية أمن البيانات والمعلومات:

١. إنشاء كلمات سر قوية.
٢. تغيير كلمات السر بانتظام.
٣. عدم استخدام كلمات سر متكررة.

تهديدات الأمن السيبراني:

- **الحدث الأبرز الذي أظهر أهمية وجود أمن سيبراني: تعرضت شركة Yahoo لأكبر اختراقات البيانات في التاريخ.**
- **ما ترتب على هذا الحدث:**
  ١. أثر بشكل كبير في سمعة الشركة.
  ٢. خسائر مالية ضخمة.
- **أهداف الأمن السيبراني:**
  ١. حماية البيانات.

٢. توافر الخدمة.
٣. الخصوصية.

- المقصود بتهديدات الأمن السيبراني: هي محاولات أو إجراءات خبيثة تهدف إلى إلحاق الضرر بأنظمة المعلومات أو الشبكات أو البيانات الخاصة بالمؤسسات أو الأفراد.
- أبرز مشكلات الأمن السيبراني:

١. البرامج الخبيثة: هي برامج ضارة تصيب الأنظمة الحاسوبية بهدف التدمير أو التجسس أو سرقة البيانات.
   - مثال على البرامج الخبيثة: برامج الفدية (برامج تقفل الأنظمة وتشفر البيانات وتطلب فدية لإعادتها).
٢. التصيد الاحتيالي: محاولات احتيالية للحصول على معلومات حساسة عن طريق تقمص هوية جهات موثوقة عبر البريد الالكتروني أو الرسائل النصية أو المواقع المزيفة.
٣. الثغرات الأمنية: هي نقاط ضعف أو عيوب في الأنظمة أو البرامج أو الشبكات يمكن أن تستغل من قبل المهاجمين لاختراق النظام والوصول إلى بيانات حساسة أو القيام بتصرفات ضارة.
   - مثال على ثغرات أمنية: ثغرات البرمجيات.
٤. حجب الخدمة الموزعة: نوع من الهجمات يتم فيه إغراق نظام أو خادم معين بعدد هائل من الطلبات بشكل متزامن من مصادر موزعة عدة بهدف إيقاف عمل النظام أو جعله غير قادر على الاستجابة للمستخدمين الشرعيين.
٥. سرقة الهوية: استخدام معلومات شخصية مسروقة لتمثيل شخص آخر دون إذنه.
   - مثال على طريقة لسرقة الهوية: التصفح غير الآمن.
٦. الهندسة الاجتماعية: هي تقنية احتيالية تعتمد على التلاعب النفسي بالأفراد لاستدراجهم للكشف عن معلومات حساسة أو القيام بأفعال معينة تساعد المهاجمين على اختراق الأنظمة أو سرقة البيانات.
   - إجراءات الهندسة الاجتماعية:
     ١. جمع المعلومات.
     ٢. بناء الثقة.
     ٣. استغلال الثقة.

٤. تنفيذ الهجوم.

- **الفرق بين الهجوم الإلكتروني والاعتداء الإلكتروني:**
  ١. الهجوم الإلكتروني هو أي نشاط غير مشروع.
  ٢. الهجوم الإلكتروني أشمل من الاعتداء الإلكتروني.
  ٣. الاعتداء الإلكتروني يضمن ضرر في جزء من النظام بشكل فوري (تركيز على التسبب في ضرر مباشر).

وسائل الحماية من تهديدات الأمن السيبراني:

١. الحماية المادية.
٢. الحماية الرقمية.

التكامل الوظيفي بين الوسائل المادية والرقمية لحماية البيانات المتبادلة يشمل:

١. الأمان المادي.
٢. الأمان الرقمي.
٣. الممارسات الجيدة للأمان.

الحماية المادية للأجهزة:

- تتم من خلال استخدام وحدات تخزين وأقفال الأمان وأنظمة المراقبة لمنع الوصول غير المصرح به إلى الأجهزة التي تخزن البيانات.