مدارس العلوم التطبيقية	**ملخص الاختبار الاول** العـام الدراسي 2025/2024 م الأمن السيبرانيّ	التاريخ : / 2/ 2025م
هاتف 5240960		الموضوع : المهارات الرقمية
اسم الطالب/ـة :		الصف : التاسع الأساسي (أ،ب) الفصل الدراسي الثاني معلمة المادة: آلاء الحوراني

المواطنة الرقمية :

ما هي أشكال البيانات؟

1. كميّة **2. نوعيّة** **3. مجردة**

ما هو سبب ظهور أمن المعلومات :

أهمية المعلومات في اتخاذ القرارات.

أمن المعلومات:

مجموعة من الاجراءات و التدابير الأمنية التي تشمل السياسات و الاجراءات و التقنيات التي تحمي المعلومات الحساسة من سوء الاستخدام أو الوصول غير المصرّح به أو التعطيل أو الاتلاف.

أهمية أمن البيانات فيما يلي:

1. الحفاظ على الخصوصية :

حماية البيانات الشخصية و الحسّسة من الوصول غير المصرّح.

2. ضمان التوافر :

ضمان أن المعلومات متاحة عند الحاجة إليها .

3. الامتثال للقوانين:

من الأمثلة على تشريعات تُلزم المؤسسات بحماية بيانات العملاء:

1. CCPA **2. GDPR**

ملاحظات هامة:

1. **أمن المعلومات يشمل الأمن السيبرانيّ**
2. **الأمن السيبرانيّ أوسع مجال من أمن المعلومات**

الأمن السيبرانيّ :

هو الحماية و الوقاية من الأخطار و التهديدات الموجودة في الفضاء الالكتروني أو الفضاء السيبرانيّ الذي يشمل الانترنت و الشبكات الرقميّة.

ما هي العناصر الرئيسية لسياسة أمن المعلومات و الأمن السيبرانيّ:

1. **أمن التطبيقات:**

النهج و الاجراءات و الأدوات و أفضل الممارسات التي توضع لحماية التطبيقات و بياناتها.

2. **التعافي من الكارثة :**

طريقة لإعادة إنشاء أنظمة تكنولوجية فعّالة في أعقاب حدث و النسخ الاحتياطي المنتظم للبيانات.

3. **أمن البنية التحتية :**

الأمان الذي يشمل البنية التحتيّة التكنولوجية (الأجهزة الرقميّة و البرامج)

ما هي الركائز الثلاث لأمن المعلومات :

1. **السرّية**
2. **التوافر**
3. **النزاهة**

ما هي أفضل الممارسات لاستخدام كلمة السّر لحماية أمن البيانات و المعلومات:

1. **إنشاء كلمات سر قويّة.**
2. **تغيير كلمات السّر بانتظام .**
3. **عدم استخدام كلمات سر متكررة.**

تهديدات الأمن السيبرانيّ :

ما هو الحدث الأبرز الذي أظهر أهمية وجود أمن سيبراني ؟

تعرضت شركة Yahoo إلى أكبر اختراقات البيانات في التاريخ.

ماذا ترتّب على هذا الحدث ؟

1. أثّر بشكل كبير في سمعة الشّركة .

2. خسائر مالية ضخمة .

إلى ماذا يهدف الأمن السيبرانيّ(أهداف الأمن السيبرانيّ) ؟

1. حماية البيانات .

2. توافر الخدمة .

3. الخصوصيّة .

ما المقصود بتهديدات الأمن السيبرانيّ؟

هي محاولات أو اجراءات خبيثة تهدف إلى إلحاق الضرر بأنظمة المعلومات أو الشبكات أو البيانات الخاصة بالمؤسسات او الأفراد .

ما هي أبرز مشكلات الأمن السيبرانيّ؟

1. البرامج الخبيثة :

هي برامج ضارّة تصيب الأنظمة الحاسوبية بهدف التدمير أو التجسس أو سرقة البيانات .

مثال على البرامج الخبيثة :

((((برامج الفدية : برامج تقفل الأنظمة و تشفّر البيانات و تطلب فدية لإعادتها .)))) حفظ مبدأ عملها

2. التصيّد الاحتيالي :

محاولات احتيالية للحصول على معلومات حساسة عن طريق تقمّص هويّة جهات موثوقة عبر البريد الالكتروني أو الرسائل النصيّة أو المواقع المزيّفة .

3. الثّغرات الأمنيّة:

هي نقاط ضعف أو عيوب في الأنظمة أو البرامج أو الشبكات يمكن أن تُستغل من قبل المهاجمين لاختراق النّظام و الوصول إلى بيانات حسّاسة أو القيام بتصرّفات ضارّة.

مثال على ثغرات أمنيّة :(ثغرات البرمجيّات)

4. حجب الخدمة الموزّعة :

نوع من الهجمات يتم فيه إغراق نظام أو خادم معيّن بعدد هائل من الطلبات بشكل متزامن من مصادر موزّعة عدّة بهدف إيقاف عمل النّظام أو جعله غير قادر على الاستجابة للمستخدمين الشّرعيين .

5. سرقة الهويّة:

استخدام معلومات شخصيّة مسروقة لتمثيل شخص آخر دون إذنه.

مثال على طريقة لسرقة الهويّة : (التّصفّح غير الآمن) .

6. الهندسة الاجتماعيّة:

هي تقنيّة احتياليّة تعتمد على التّلاعب النّفسي بالأفراد لاستدراجهم للكشف عن معلومات حسّاسة أو القيام بأفعال معيّنة تساعد المهاجمين على اختراق الأنظمة أو سرقة البيانات.

اجراءات الهندسة الاجتماعية :

1. **جمع المعلومات.**
2. **بناء الثّقة .**
3. **استغلال الثّقة .**
4. **تنفيذ الهجوم .**

ما الفرق بين الهجوم الإلكترونيّ و الاعتداء الإلكترونيّ :

1. **الهجوم الإلكتروني هو أيّ نشاط غير مشروع .**
2. **الهجوم الإلكتروني أشمل من الاعتداء الإكترونيّ.**
3. **الاعتداء الإلكترونيّ يضمن ضرر في جزء من النّظام بشكل فوريّ (تركيز على التّسبّب في ضرر مباشر)**

وسائل الحماية من تهديدات الأمن السيبرانيّ:

1. **الحماية الماديّة.**
2. **الحماية الرّقميّة.**

ماذا يشمل التكامل الوظيفيّ بين الوسائل الماديّة و الرّقميّة لحماية البيانات المتبادلة :

1. **الأمان الماديّ.**
2. **الأمان الرقميّ.**
3. **الممارسات الجيّدة للأمان.**

كيف تتم الحماية الماديّة للأجهزة ؟

من خلال استخدام وحدات تخزين و أقفال الأمان و أنظمة المراقبة لمنع الوصول غير المصرّح به إلى الأجهزة التي تُخزّن البيانات.

انتهى الملخص