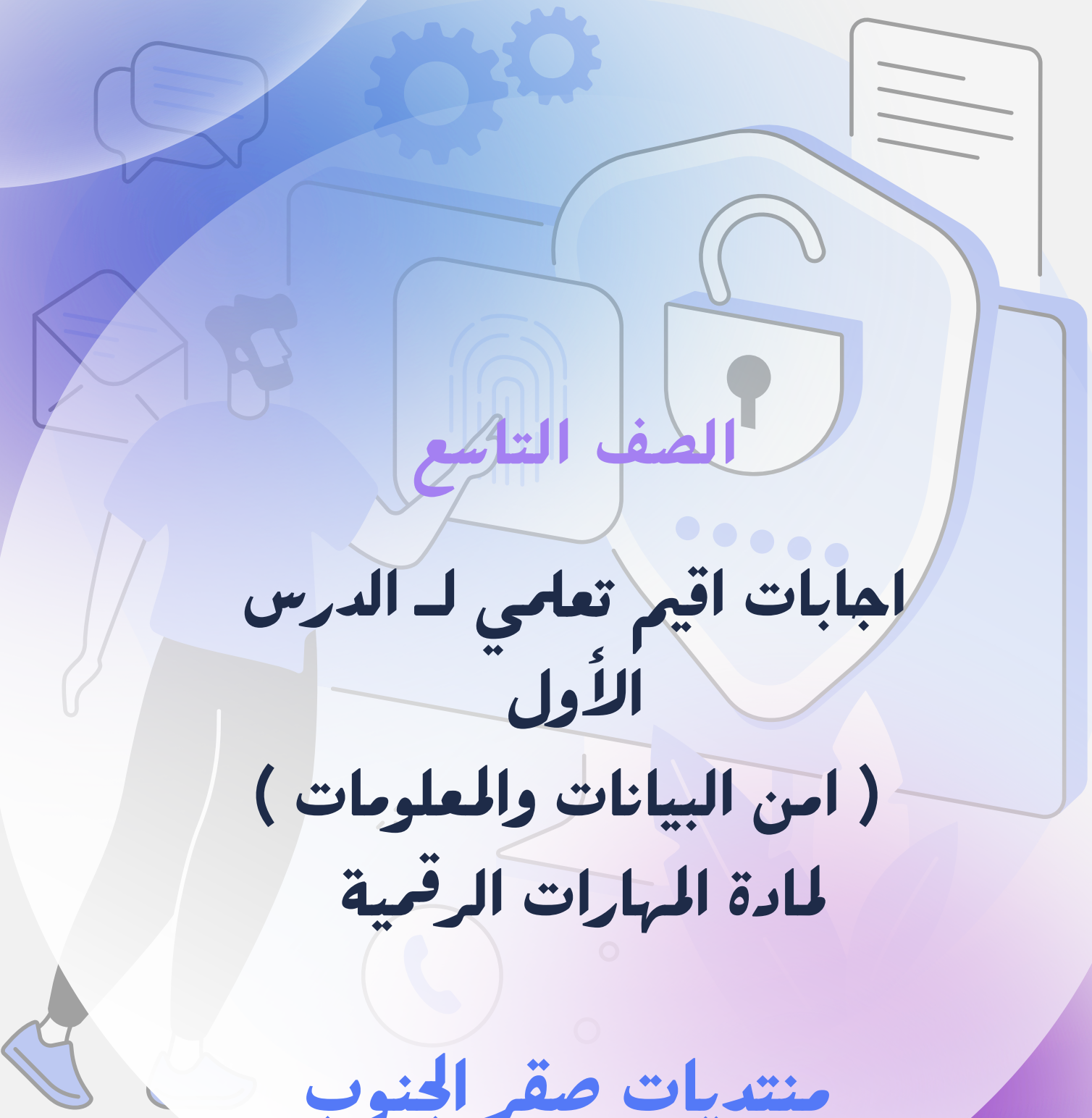

الصف التاسع

اجابات اقيم تعلمي لـ الدرس الأول
(امن البيانات والمعلومات)
لمادة المهارات الرقمية

منتديات صقر الجنوب

أقيِّم تعلُّمي — الدرس الأول (أمن البيانات والمعلومات)

المعرفةُ: استخدمُ ما تعلمتَهُ منْ معارفَ في هذا الدرسِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السؤالُ الأولُ: أقارنُ بينَ أمنِ المعلوماتِ والأمنِ السيبرانيِّ.

يمكن الاختلاف بين امن المعلومات والأمن السيبراني في تركيز أمن المعلومات بشكل اساسي على حماية البيانات والمعلومات بغض النضر عن مكانها (سواء اكانت على الورق أو في الانظمة الرقمية)

السؤالُ الثاني: أبيّنُ العناصرَ الرئيسةَ لسياسةِ أمنِ المعلوماتِ.

1. **أمنَ التطبيقاتِ (Application Security):** النهجُ والإجراءاتُ والأدواتُ وأفضلُ الممارساتِ التي توضعُ لحمايةِ التطبيقاتِ وبياناتِها. يمكنُ استخدامُ أدواتِ فحصِ الثغراتِ، مثلَ Burp Suite.

2. **الأمنَ السحابيَّ (Cloud Security):** النهجُ والإجراءاتُ والأدواتُ وأفضلُ الممارساتِ التي توضعُ لحمايةِ السحابةِ ككلٍّ، بما في ذلكَ الأنظمةُ والبياناتُ والتطبيقاتُ والبنيةُ الأساسيةُ. ويتضمنُ تشفيرَ البياناتِ، والتحكمِ في الوصولِ، ومراقبةَ الأنشطةِ عبرَ السحابةِ.

3. **التّعافي منَ الكارثةِ (Disaster Recovery):** طريقةٌ لإعادةِ إنشاءِ أنظمةٍ تكنولوجيةٍ فعالةٍ في أعقابِ حدثٍ، مثلَ كارثةٍ طبيعيةٍ أوْ هجومٍ إلكترونيٍّ أوْ حدثٍ تخريبيٍّ آخرَ. ويتضمنُ تطويرَ خطةِ التعافي منَ الكوارثِ والنسخِ الاحتياطيِّ المنتظمِ للبياناتِ.

4. **الاستجابةَ للحوادثِ (Incident Response):** خطةٌ للاستجابةِ لتداعياتِ أيِّ هجومٍ عبرَ الإنترنتْ أوْ تسربٍ للبياناتِ أوْ حدثٍ تخريبيٍّ آخرَ، ومعالجتِهِ وإدارتِهِ. ويتضمنُ استخدامَ أدواتِ تحليلِ الأمانِ، مثلَ نظامِ إدارةِ المعلوماتِ والأحداثِ الأمنيةِ (SIEM) لرصدِ الحوادثِ الأمنيةِ وتحليلِها.

5. **أمنَ البنيةِ التحتيةِ (Infrastructure Security):** الأمانُ الذي يشملُ البنيةَ التحتيةَ التكنولوجيةَ، بما في ذلكَ أنظمةُ الأجهزةِ والبرامجِ. ويتضمنُ تأمينَ الشبكةِ وتحديثَ الأنظمةِ بانتظامٍ وتطبيقَ قواعدِ التحكمِ في الوصولِ.

6. **إدارة الثغرات الأمنية (Vulnerability Management):** العملية التي تجريها المؤسسة لتحديد الثغرات الأمنية في نقاط النهاية والبرامج والأنظمة الخاصة بها، وتقييمها ومعالجتها.

السؤالُ الثالثُ: أوضحَ أهميةَ استخدامِ كلماتِ المرورِ لحمايةِ البياناتِ الشخصيةِ.

تبرز أهميتها في منع الوصول غير المصرح به للبيانات أو المعلومات، وحماية البيانات الحساسة، وتعزيز الخصوصية الشخصية، وحماية الأجهزة والشبكات، وهي عنصر أساسي في استراتيجيات الأمان متعددة الطبقات. وتكمن أهميتها في بيانات العمل بحماية البيانات الحساسة للعملاء، وحماية الأصول الرقمية

المهاراتُ: أوظفُ مهاراتِ التفكيرِ الناقدِ، والبحثِ الرقميِّ، والتواصلِ للإجابةِ عنِ الأسئلةِ الآتيةِ:

السـؤالُ الأولُ: أبحثُ في طرقِ الحفاظِ على أمـنِ المعلوماتِ الحديثةِ، وأدونُها في مستندِ Google Docs.

1. التشفير: استخدام RSA و AES-256 لحماية البيانات.
2. المصادقة المتعددة (MFA): إضافة طبقات أمان مثل البصمة والرسائل النصية.
3. الذكاء الاصطناعي: اكتشاف التهديدات تلقائيًا عبر AI و ML.
4. تحديث الأنظمة: تثبيت التحديثات الأمنية فور صدورها.
5. الحماية من التصيد: تدريب الموظفين واستخدام البريد الإلكتروني الآمن.
6. تأمين الشبكات: تفعيل جدران الحماية (Firewalls) وأنظمة كشف التسلل (IDS/IPS).
7. النسخ الاحتياطي: حفظ نسخ دورية من البيانات وفق استراتيجية 3-2-1.
8. التحكم في الوصول: تطبيق Zero Trust لتقييد الصلاحيات.
9. أمان السحابة: استخدام تشفير للبيانات السحابية وإدارة الأدوات.
10. اختبار الاختراق: فحص الثغرات بأدوات مثل Nmap و Burp Suite.
11. التوعية الأمنية: تدريب الموظفين للحد من الأخطاء البشرية.
12. إدارة الحوادث: وضع خطة استجابة سريعة واستخدام أنظمة SIEM.
13. الحماية البيومترية: استخدام بصمات الأصابع والتعرف على الوجه.
14. أمان الإنترنت اللاسلكي: تفعيل الأنظمة الحديثة مثل WPA3.
15. إدارة كلمات المرور: استخدام مديري كلمات المرور وتقنية WebAuthn."

السؤالُ الثاني: أفكرُ في طرقٍ برمجيةٍ لإنشاءِ كلماتِ المرورِ وتغييرِها بشكلٍ دوريٍّ.

يترك للطالب

الســـؤالُ الثالثُ: هلْ أتوقعُ أنْ تكونَ المعلوماتُ في المســـتقبلِ الرقميِّ وتطوراتِهِ المتسارعةِ أكثرَ أمانًا؟ أفسرُ إجابتي.

"لا يمكن الجزم بأن المعلومات ستكون أكثر أماناً في المستقبل الرقمي، حيث يعتمد ذلك على توازن بين تطور تقنيات الحماية وتطور الهجمات الإلكترونية.

1. تحسينات في الأمن السيبراني:
- تقدم تقنيات الذكاء الاصطناعي والتشفير الكمي والمصادقة البيومترية ستجعل حماية المعلومات أقوى.
- انتشار تقنيات Zero Trust وأمن السحابة المتقدم يعزز الأمان.

2. تطور التهديدات الإلكترونية:
- مع تطور التقنية، تصبح الهجمات أكثر تعقيداً، مثل الهجمات باستخدام الذكاء الاصطناعي والبرمجيات الخبيثة المتقدمة.
- ظهور الاختراقات الكمية قد يجعل التشفير التقليدي غير فعال.

3. عامل الخطأ البشري:
- يبقى الإهمال البشري والتوعية الأمنية الضعيفة من أكبر الثغرات الأمنية.
- الهندسة الاجتماعية والتصيد الاحتيالي ستظل تهديدات قائمة."