السؤال الأول ضع دائرة حول رمز الإجابة الصحيحة :

1. ما المقصود بأمن البيانات والمعلومات؟

أ) حماية الأجهزة فقط من الفيروسات

ب) مجموعة تدابير تحمي البيانات من الوصول غير المصرح به أو التعديل أو التدمير

ج) استخدام كلمات مرور قوية فقط

د) مشاركة البيانات مع جميع المستخدمين

2. ما الفرق الأساسي بين أمن المعلومات والأمن السيبراني؟

أ) أمن المعلومات يركز على حماية البيانات، بينما الأمن السيبراني يركز على حماية الأنظمة والشبكات

ب) الأمن السيبراني يهتم فقط بحماية الحسابات الشخصية

ج) أمن المعلومات يتعلق فقط بالتشفير

د) لا يوجد فرق بينهما

3. ما هي الركائز الثلاث لأمن المعلومات؟

أ) التشفير، المصادقة الثنائية، التخزين السحابي

ب) الخصوصية، الأمان، الحماية

ج) السرية، النزاهة، التوافر

د) التحكم في الوصول، كلمات المرور، برامج مكافحة الفيروسات

4. أي من الخيارات التالية يعبر عن السرية (Confidentiality) في أمن المعلومات؟

أ) التأكد من أن المعلومات لم تتغير أثناء تخزينها أو نقلها

ب) السماح فقط للمستخدمين المخوّلين بالوصول إلى المعلومات

ج) الاحتفاظ بنسخ احتياطية من البيانات

د) التأكد من أن البيانات متاحة عند الحاجة إليها

5. ما هي أحد أمثلة النزاهة (Integrity) في أمن المعلومات؟

أ) التحقق من عدم تعديل البيانات بشكل غير قانوني

ب) ضمان توفر البيانات دائمًا عند الحاجة إليها

ج) السماح لأي شخص بالوصول إلى المعلومات

د) حذف البيانات بشكل دوري لمنع الوصول غير المصرح به

6. ما هو أحد أمثلة التوافر (Availability) في أمن المعلومات؟

أ) استخدام التشفير لحماية البيانات

ب) ضمان أن تكون البيانات متاحة عند الحاجة إليها

ج) منع المستخدمين من الوصول إلى المعلومات

د) استخدام جدران الحماية لمنع الهجمات الإلكترونية

7. أي من الخيارات التالية يعد مثالاً على أمن المعلومات وليس الأمن السيبراني؟

أ) استخدام جدار حماية لحماية الشبكة

ب) استخدام كلمات مرور قوية لحماية الحسابات الشخصية

ج) تثبيت برامج مكافحة الفيروسات

د) تفعيل المصادقة الثنائية لحسابات البريد الإلكتروني

8. ما أهمية كلمات المرور القوية في أمن المعلومات؟

أ) تمنع الوصول غير المصرح به إلى البيانات

ب) تجعل تسجيل الدخول أسهل

ج) تُستخدم لحماية الملفات فقط

د) لا تؤثر على أمان البيانات

9. أي من الخيارات التالية ليس من عناصر سياسة أمن المعلومات؟

أ) أمن التطبيقات

ب) أمن السحابة

ج) ترك الأجهزة غير محمية بكلمة مرور

د) الاستجابة للحوادث الأمنية

10. ما أفضل طريقة لإنشاء كلمة مرور قوية؟

أ) استخدام نفس كلمة المرور لكل الحسابات

ب) اختيار كلمة مرور قصيرة وسهلة التذكر

ج) استخدام مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز

د) كتابة كلمة المرور على ورقة بجانب الحاسوب

11. ما أحد أهم أهداف أمن المعلومات؟

أ) منع الأشخاص من استخدام الإنترنت

ب) الحفاظ على سرية ونزاهة وتوافر المعلومات

ج) تقليل عدد المستخدمين في الشبكة

د) حذف البيانات بشكل دوري

12. أي من الخيارات التالية يعد جزءًا من سياسة التعافي من الكوارث (Disaster Recovery)؟

أ) إنشاء جدار حماية لحماية الشبكة

ب) إعداد خطط لاستعادة البيانات بعد الهجمات أو الكوارث الطبيعية

ج) استخدام التشفير لحماية الملفات

د) تثبيت برامج مكافحة الفيروسات

13. لماذا تعتبر إدارة الثغرات الأمنية (Vulnerability Management) مهمة في أمن المعلومات؟

أ) لتحديد وإصلاح الثغرات قبل أن يستغلها القراصنة

ب) لتسهيل اختراق الأنظمة بسهولة

ج) لمنع المستخدمين من تغيير كلمات المرور الخاصة بهم

د) لزيادة عدد البرامج الضارة في النظام

14. ما هو الهدف من التشفير (Encryption) في أمن البيانات؟

أ) جعل البيانات غير قابلة للقراءة إلا للأشخاص المخوّلين

ب) حذف جميع البيانات الحساسة تلقائيًا

ج) تسريع عملية الوصول إلى البيانات

د) مشاركة المعلومات الحساسة مع الجميع

15. ما هو أحد الأسباب الشائعة لاختراق الحسابات الشخصية؟

أ) استخدام كلمة مرور قصيرة وسهلة التخمين

ب) استخدام المصادقة الثنائية (2FA)

ج) تجنب فتح الروابط المشبوهة

د) تحديث كلمات المرور بانتظام

16. كيف يمكن حماية البيانات على الأجهزة المحمولة؟

أ) عدم قفل الهاتف مطلقًا

ب) استخدام كلمات مرور قوية وتمكين تشفير البيانات

ج) مشاركة جميع البيانات مع التطبيقات غير الموثوقة

د) تثبيت أي تطبيق دون مراجعة الأذونات

17. ما هو أحد العناصر الرئيسية لسياسة أمن المعلومات؟

أ) استخدام كلمات مرور ضعيفة.

ب) إدارة الثغرات الأمنية.

ج) عدم تحديث الأنظمة بانتظام.

د) عدم استخدام التشفير.

18. ما هو أحد التهديدات الشائعة للأمن السيبراني؟

أ) استخدام كلمات مرور قوية.

ب) الهجمات الإلكترونية مثل البرمجيات الضارة.

ج) تحديث أنظمة التشغيل بانتظام.

د) استخدام التشفير لحماية البيانات.

19. هناك العديد من القوانين التي تلزم الشركات حماية بيانات العملاء مثل

أ) قانون حماية المستهلك .

ب) اللائحة العامة لحماية البيانات.

ج) قانون الملكية الفكرية.

د) أ+ ب.

20. المصطلح الذي يشير الى انترنت الاشياء هو

أ) IoT

ب) CCPA.

ج) DoS.

د) GDPR

21. العنصر المسؤول عن فحص الثغرات

أ) الاستجابة للحوادث الأمنية.

ب) أمن التطبيقات.

ج) الأمن السحابي.

د) أمن البنية التحتية

22. .....يتضمن تشفير البيانات والتحكم بالوصول اليها

أ) الاستجابة للحوادث الأمنية.

ب) أمن التطبيقات.

ج) الأمن السحابي.

د) أمن البنية التحتية

23. يهتم امن البنية التحتية بتأمين الأجهزة والشبكات وقواعد البيانات من الهجمات الإلكترونية

أ) صح ب) خطأ

24. يفضل عدم تغيير كلمة السر الا عند الضرورة الشديدة

أ) صح ب) خطأ

25. أمن المعلومات يركز على حماية البيانات والمعلومات بغض النظر عن الوسيط المستخدم سواء كان ذلك عبر الإنترنت أو على الورق أو في قواعد البيانات

أ) صح ب) خطأ

السؤال الثاني | ما الفرق بين أمن المعلومات والأمن السيبراني؟

أمن المعلومات يركز على حماية البيانات نفسها، سواء كانت مخزنة رقميًا أو على ورق، بغض النظر عن الوسيلة المستخدمة في تخزينها أو نقلها.

الأمن السيبراني هو مجال أوسع يشمل حماية الأنظمة والشبكات والأجهزة المتصلة بالإنترنت من الهجمات الإلكترونية، ويغطي جوانب مثل أمن الشبكات، أمن التطبيقات، وأمن السحابة.

السؤال الثالث: ما هي الركائز الثلاث الأساسية لأمن المعلومات؟

يعتمد أمن المعلومات على ثلاث ركائز رئيسية تُعرف باسم مثلث CIA وهي:

1. السرية:(Confidentiality)
   - تعني حماية البيانات من الوصول غير المصرح به.
2. النزاهة:(Integrity)
   - تعني التأكد من أن البيانات لم يتم تغييرها أو التلاعب بها دون إذن.
3. التوافر:(Availability)
   - ضمان إمكانية الوصول إلى البيانات والمعلومات عند الحاجة إليها.

السؤال الرابع: ما أهمية استخدام كلمات المرور القوية؟ وكيف يمكن إنشاء كلمة مرور آمنة؟

تعد كلمات المرور القوية خط الدفاع الأول لحماية الحسابات والبيانات، حيث تمنع الوصول غير المصرح به، وتقلل من احتمالية تعرض البيانات للاختراق.

لإنشاء كلمة مرور آمنة، يجب اتباع المعايير التالية:

1. الطول :يجب ألا تقل عن 12-16 حرفًا.
2. التنوع :يجب أن تحتوي على أحرف كبيرة وصغيرة، أرقام، ورموز خاصة مثل.(*&^%#@!)
3. عدم استخدام كلمات مرور شائعة :مثل "password123" أو "123456."
4. تغييرها بانتظام :يوصى بتغييرها كل 3-6 أشهر.
5. عدم استخدامها في أكثر من حساب واحد :لتقليل المخاطر في حال تم اختراق أحد الحسابات

السؤال الأول ضع دائرة حول رمز الإجابة الصحيحة :

1. ما المقصود بأمن البيانات والمعلومات؟

أ) حماية الأجهزة فقط من الفيروسات

ب) مجموعة تدابير تحمي البيانات من الوصول غير المصرح به أو التعديل أو التدمير

ج) استخدام كلمات مرور قوية فقط

د) مشاركة البيانات مع جميع المستخدمين

2. ما الفرق الأساسي بين أمن المعلومات والأمن السيبراني؟

أ) أمن المعلومات يركز على حماية البيانات، بينما الأمن السيبراني يركز على حماية الأنظمة والشبكات

ب) الأمن السيبراني يهتم فقط بحماية الحسابات الشخصية

ج) أمن المعلومات يتعلق فقط بالتشفير

د) لا يوجد فرق بينهما

3. ما هي الركائز الثلاث لأمن المعلومات؟

أ) التشفير، المصادقة الثنائية، التخزين السحابي

ب) الخصوصية، الأمان، الحماية

ج) السرية، النزاهة، التوافر

د) التحكم في الوصول، كلمات المرور، برامج مكافحة الفيروسات

4. أي من الخيارات التالية يعبر عن السرية (Confidentiality) في أمن المعلومات؟

أ) التأكد من أن المعلومات لم تتغير أثناء تخزينها أو نقلها

ب) السماح فقط للمستخدمين المخوّلين بالوصول إلى المعلومات

ج) الاحتفاظ بنسخ احتياطية من البيانات

د) التأكد من أن البيانات متاحة عند الحاجة إليها

5. ما هي أحد أمثلة النزاهة (Integrity) في أمن المعلومات؟

أ) التحقق من عدم تعديل البيانات بشكل غير قانوني

ب) ضمان توفر البيانات دائمًا عند الحاجة إليها

ج) السماح لأي شخص بالوصول إلى المعلومات

د) حذف البيانات بشكل دوري لمنع الوصول غير المصرح به

6. ما هو أحد أمثلة التوافر (Availability) في أمن المعلومات؟

أ) استخدام التشفير لحماية البيانات

ب) ضمان أن تكون البيانات متاحة عند الحاجة إليها

ج) منع المستخدمين من الوصول إلى المعلومات

د) استخدام جدران الحماية لمنع الهجمات الإلكترونية

7. أي من الخيارات التالية يعد مثالاً على أمن المعلومات وليس الأمن السيبراني؟

أ) استخدام جدار حماية لحماية الشبكة

ب) استخدام كلمات مرور قوية لحماية الحسابات الشخصية

ج) تثبيت برامج مكافحة الفيروسات

د) تفعيل المصادقة الثنائية لحسابات البريد الإلكتروني

8. ما أهمية كلمات المرور القوية في أمن المعلومات؟

أ) تمنع الوصول غير المصرح به إلى البيانات

ب) تجعل تسجيل الدخول أسهل

ج) تُستخدم لحماية الملفات فقط

د) لا تؤثر على أمان البيانات

9. أي من الخيارات التالية ليس من عناصر سياسة أمن المعلومات؟

أ) أمن التطبيقات

ب) أمن السحابة

ج) ترك الأجهزة غير محمية بكلمة مرور

د) الاستجابة للحوادث الأمنية

10. ما أفضل طريقة لإنشاء كلمة مرور قوية؟

أ) استخدام نفس كلمة المرور لكل الحسابات

ب) اختيار كلمة مرور قصيرة وسهلة التذكر

ج) استخدام مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز

د) كتابة كلمة المرور على ورقة بجانب الحاسوب

11. ما أحد أهم أهداف أمن المعلومات؟

أ) منع الأشخاص من استخدام الإنترنت

ب) الحفاظ على سرية ونزاهة وتوافر المعلومات

ج) تقليل عدد المستخدمين في الشبكة

د) حذف البيانات بشكل دوري

12. أي من الخيارات التالية يعد جزءًا من سياسة التعافي من الكوارث (Disaster Recovery)؟

أ) إنشاء جدار حماية لحماية الشبكة

ب) إعداد خطط لاستعادة البيانات بعد الهجمات أو الكوارث الطبيعية

ج) استخدام التشفير لحماية الملفات

د) تثبيت برامج مكافحة الفيروسات

13. لماذا تعتبر إدارة الثغرات الأمنية (Vulnerability Management) مهمة في أمن المعلومات؟

أ) لتحديد وإصلاح الثغرات قبل أن يستغلها القراصنة

ب) لتسهيل اختراق الأنظمة بسهولة

ج) لمنع المستخدمين من تغيير كلمات المرور الخاصة بهم

د) لزيادة عدد البرامج الضارة في النظام

14. ما هو الهدف من التشفير (Encryption) في أمن البيانات؟

أ) جعل البيانات غير قابلة للقراءة إلا للأشخاص المخوّلين

ب) حذف جميع البيانات الحساسة تلقائيًا

ج) تسريع عملية الوصول إلى البيانات

د) مشاركة المعلومات الحساسة مع الجميع

15. ما هو أحد الأسباب الشائعة لاختراق الحسابات الشخصية؟

أ) استخدام كلمة مرور قصيرة وسهلة التخمين

ب) استخدام المصادقة الثنائية (2FA)

ج) تجنب فتح الروابط المشبوهة

د) تحديث كلمات المرور بانتظام

16. كيف يمكن حماية البيانات على الأجهزة المحمولة؟

أ) عدم قفل الهاتف مطلقًا

ب) استخدام كلمات مرور قوية وتمكين تشفير البيانات

ج) مشاركة جميع البيانات مع التطبيقات غير الموثوقة

د) تثبيت أي تطبيق دون مراجعة الأذونات

17. ما هو أحد العناصر الرئيسية لسياسة أمن المعلومات؟

أ) استخدام كلمات مرور ضعيفة.

ب) إدارة الثغرات الأمنية.

ج) عدم تحديث الأنظمة بانتظام.

د) عدم استخدام التشفير.

18. ما هو أحد التهديدات الشائعة للأمن السيبراني؟

أ) استخدام كلمات مرور قوية.

ب) الهجمات الإلكترونية مثل البرمجيات الضارة.

ج) تحديث أنظمة التشغيل بانتظام.

د) استخدام التشفير لحماية البيانات.

19. هناك العديد من القوانين التي تلزم الشركات حماية بيانات العملاء مثل

أ) قانون حماية المستهلك .

ب) اللائحة العامة لحماية البيانات.

ج) قانون الملكية الفكرية.

د) أ+ ب.

20. المصطلح الذي يشير الى انترنت الاشياء هو

ب) IoT

ب) CCPA.

ج) DoS.

د) GDPR

21. العنصر المسؤول عن فحص الثغرات

أ) الاستجابة للحوادث الأمنية.

ب) أمن التطبيقات.

ج) الأمن السحابي.

د) أمن البنية التحتية

22. .....يتضمن تشفير البيانات والتحكم بالوصول اليها

أ) الاستجابة للحوادث الأمنية.

ب) أمن التطبيقات.

ج) الأمن السحابي.

د) أمن البنية التحتية

23. يهتم امن البنية التحتية بتأمين الأجهزة والشبكات وقواعد البيانات من الهجمات الإلكترونية

أ) صح ب) خطأ

24. يفضل عدم تغيير كلمة السر الا عند الضرورة الشديدة

أ) صح ب) خطأ

25. أمن المعلومات يركز على حماية البيانات والمعلومات بغض النظر عن الوسيط المستخدم سواء كان ذلك عبر الإنترنت أو على الورق أو في قواعد البيانات

أ) صح ب) خطأ

السؤال الثاني ما الفرق بين أمن المعلومات والأمن السيبراني؟

أمن المعلومات يركز على حماية البيانات نفسها، سواء كانت مخزنة رقميًا أو على ورق، بغض النظر عن الوسيلة المستخدمة في تخزينها أو نقلها.

الأمن السيبراني هو مجال أوسع يشمل حماية الأنظمة والشبكات والأجهزة المتصلة بالإنترنت من الهجمات الإلكترونية، ويغطي جوانب مثل أمن الشبكات، أمن التطبيقات، وأمن السحابة.

السؤال الثالث: ما هي الركائز الثلاث الأساسية لأمن المعلومات؟

يعتمد أمن المعلومات على ثلاث ركائز رئيسية تُعرف باسم مثلث CIA وهي:

4. السرية:(Confidentiality)
   - تعني حماية البيانات من الوصول غير المصرح به.
5. النزاهة:(Integrity)
   - تعني التأكد من أن البيانات لم يتم تغييرها أو التلاعب بها دون إذن.
6. التوافر:(Availability)
   - ضمان إمكانية الوصول إلى البيانات والمعلومات عند الحاجة إليها.

السؤال الرابع: ما أهمية استخدام كلمات المرور القوية؟ وكيف يمكن إنشاء كلمة مرور آمنة؟

تعد كلمات المرور القوية خط الدفاع الأول لحماية الحسابات والبيانات، حيث تمنع الوصول غير المصرح به، وتقلل من احتمالية تعرض البيانات للاختراق.

لإنشاء كلمة مرور آمنة، يجب اتباع المعايير التالية:

6. الطول :يجب ألا تقل عن 12-16 حرفًا.
7. التنوع :يجب أن تحتوي على أحرف كبيرة وصغيرة، أرقام، ورموز خاصة مثل.(*&^%#@!)
8. عدم استخدام كلمات مرور شائعة :مثل "password123" أو "123456."
9. تغييرها بانتظام :يوصى بتغييرها كل 3-6 أشهر.
10. عدم استخدامها في أكثر من حساب واحد :لتقليل المخاطر في حال تم اختراق أحد الحسابات