

## ✓الاختبار الشامل – الأمن السيبراني

□ القسم الأول: اختيارات من متعدد (اختر الإجابة الصحيحة)

١. ما الهدف الرئيسي من أمن المعلومات؟  
(أ) تسهيل مشاركة البيانات  
(ب) حماية البيانات من الوصول غير المصرح به  
(ج) تسريع نقل البيانات  
(د) استخدام الإنترنت بحرية

✓الإجابة: ب

٢. أي من التالي يُعدّ تهديداً سيبرانياً؟  
(أ) استخدام برنامج حماية  
(ب) المصادقة الثنائية  
(ج) التصيد الإلكتروني  
(د) تشفير البيانات

✓الإجابة: ج

٣. ما هو أفضل وصف لكلمة مرور قوية؟  
(أ) اسم المستخدم  
(ب) كلمة سهلة مثل "١٢٣٤"  
(ج) مزيج من حروف وأرقام ورموز  
(د) كلمة تحتوي على اسمك الشخصي

✓الإجابة: ج

٤. HTTPS يشير إلى:  
(أ) بروتوكول لنقل النصوص  
(ب) بروتوكول غير آمن  
(ج) بروتوكول نقل آمن باستخدام التشفير  
(د) برنامج لمكافحة الفيروسات

✓الإجابة: ج

٥. ما نوع التشفير الذي يغير مواقع الأحرف بطريقة متعرجة؟

- أ) شيفرة قيصر
- ب) شيفرة السكك الحديدية
- ج) التشفير الرقمي
- د) الشيفرة العكسية

✓ الإجابة: ب

القسم الثاني: أسئلة قصيرة

٦. اذكر اثنين من وسائل حماية البيانات.

✓ الإجابة النموذجية:

- استخدام كلمات مرور قوية
- التشفير
- المصادقة الثنائية (2FA)

٧. ما الفرق بين أمن المعلومات والأمن السيبراني؟

✓ الإجابة:

- أمن المعلومات يهتم بحماية البيانات من أي تهديد، سواء رقمي أو غير رقمي.
- الأمن السيبراني يركز على حماية البيانات والأنظمة من الهجمات الرقمية.

٨. ما هو التصيد الإلكتروني؟ وكيف يمكن تجنبه؟

✓ الإجابة:

- هو محاولة خداع المستخدم للحصول على بياناته من خلال رسائل أو مواقع وهمية.
- يمكن تجنبه بعدم النقر على روابط غير معروفة، واستخدام التحقق الثنائي.

٩. اشرح شيفرة قيصر باختصار مع مثال.

✓ الإجابة:

- هي نوع من التشفير حيث يتم تحريك الحروف بعدد معين.
- مثال: الكلمة "CHAT" مع تحريك ٣ خانات تصبح "FKDW"

١٠. لماذا يُستخدم التشفير عند نقل البيانات؟

✓ الإجابة:

- لحماية البيانات من أن يتم قراءتها أو تعديلها من قبل جهات غير مصرح بها.