

السؤال الأول

- (Encryption) التشفير: عملية تحويل البيانات إلى صيغة غير قابلة للقراءة
- (Backup) النسخ الاحتياطي: إنشاء نسخ عند فقدان البيانات أو إتلافها وتخزينها في مكان آمن
- (Access Control) التحكم في الوصول: منح أذونات معينة للأشخاص أو الجهات المعنية فقط للوصول إلى البيانات
- (Authentication) المصادقة: التأكد من هوية الأفراد أو الأجهزة التي تطلب الوصول إلى بيانات معينة

السؤال الثاني

وجه المقارنة	التشفير	النسخ الاحتياطي
الفعالية	يحمي البيانات من الوصول غير المصرح به وقراءتها	يحمي البيانات من فقدان أو التلف، ويتيح استعادتها.
الجدوى	ضروري لحماية البيانات الحساسة، مثل المعلومات الشخصية والمالية.	ضروري لضمان استمرارية العمل، واستعادة البيانات في حالات الطوارئ.
التأثير الأخلاقي	يساهم في الحفاظ على خصوصية الأفراد وحماية معلوماتهم.	يساعد في الحفاظ على حقوق الملكية الفكرية، وحماية المعلومات الهامة للمؤسسات.

Google" التصدير إلى "جداول بيانات

السؤال الثالث

- (Access Control) التحكم في الوصول: منع وصول الأشخاص غير المصرح لهم إلى البيانات
- (Backup) النسخ الاحتياطي: ضمان توفير البيانات واستعادتها عند حدوث فقدان أو تلف للبيانات الأصلية
- (Encryption) التشفير: حماية البيانات من الوصول غير المصرح به عند نقل البيانات عبر الشبكات
- (Access Control) التحكم في الوصول: تحديد الأذونات، وتنظيم الوصول، ومنع الوصول غير المصرح به

ملاحظات

- التشفير يحول البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح فك التشفير المناسب.
- النسخ الاحتياطي يحتفظ بنسخ من البيانات في مكان آمن، مما يتيح استعادتها في حالة فقدان أو تلف البيانات الأصلية.
- التحكم في الوصول يحدد من يمكنه الوصول إلى البيانات، وما هي الصلاحيات الممنوحة لهم.
- المصادقة تتحقق من هوية المستخدمين أو الأجهزة التي تحاول الوصول إلى البيانات.

السؤال الأول: البحث عن قانون حماية البيانات الشخصية الأردني

- الخطوات:
 1. (أو محركات بحث متخصصة في القوانين Google Scholar مثل) استخدام محركات البحث الأمانة: البحث الرقمي للعثور على نص القانون. يمكنك البحث بكلمات مفتاحية مثل "قانون حماية البيانات الشخصية الأردن" أو "قانون الأمن السيبراني الأردن".
 2. التأكد من أن المواقع التي تزورها موثوقة (مثل المواقع الحكومية أو المواقع الرسمية للمنظمات: المواقع الأمانة القانونية).
 3. قراءة مواد القانون بعناية لفهم الأحكام المتعلقة بحماية البيانات الشخصية: قراءة القانون.
 4. تلخيص أهم النقاط على شكل نقاط أو فقرات قصيرة: التلخيص.

5. لتصميم بوستر جذاب يتضمن ملخص القانون مع إضافة عناصر مرئية Canva استخدام برنامج: **تصميم البوستر** مناسبة.
6. نشر البوستر على صفحة المدرسة على مواقع التواصل الاجتماعي مع استخدام هاشتاغات مناسبة: **النشر**.
- **مثال على أهم النقاط التي يمكن تلخيصها في البوستر:**
 - تعريف البيانات الشخصية وأنواعها.
 - حقوق الأفراد في التحكم في بياناتهم الشخصية (مثل حق الوصول والتعديل والحذف).
 - واجبات المؤسسات التي تجمع البيانات الشخصية (مثل الحصول على الموافقة وحماية البيانات).
 - العقوبات على مخالفة القانون.

السؤال الثاني: مستقبل التعامل مع البيانات الرقمية وحمايتها

- **توقعات حول مستقبل التعامل مع البيانات الرقمية وحمايتها:**
 - مع تطور الذكاء الاصطناعي وإنترنت الأشياء، ستصبح البيانات أكثر تعقيداً وأكثر انتشاراً، مما يزيد: **زيادة التعقيد** من صعوبة حمايتها.
 - blockchain قد نشهد ظهور تقنيات جديدة لحماية البيانات، مثل التشفير الكمي أو تقنيات: **تطورات تكنولوجيا**.
 - من المتوقع أن تزيد الحكومات من تشديد قوانين حماية البيانات لضمان خصوصية الأفراد: **تشديد القوانين**.
 - سيزداد وعي الأفراد بأهمية حماية بياناتهم الشخصية، وسيطالبون بمزيد من الشفافية والتحكم: **زيادة الوعي**.
 - ستظهر تحديات أخلاقية جديدة تتعلق باستخدام البيانات، مثل استخدامها في المراقبة أو التمييز: **تحديات أخلاقية**.
- **مشاركة التوقعات مع الزملاء:**
 - يمكن مشاركة التوقعات في نقاش مفتوح مع الزملاء، وتبادل الأفكار ووجهات النظر المختلفة.
 - يمكن أيضاً إجراء بحث إضافي حول التوجهات المستقبلية في مجال حماية البيانات، وعرض النتائج على الزملاء.

القيم والاتجاهات في الأمن السيبراني

- **جدول القيم الأخلاقية في الأمن السيبراني:**

القيم الأخلاقية التي تتعارض مع الأمن السيبراني	القيم الأخلاقية المتوافقة مع الأمن السيبراني
استخدام المعلومات بطرق مضللة أو غير أخلاقية: الخداع .	التعامل بصدق وأمانة مع البيانات والمعلومات: الأمانة .
جمع أو استخدام بيانات الأفراد دون: انتهاك الخصوصية موافقتهم.	احترام خصوصية الأفراد وحقوقهم في التحكم في بياناتهم: الاحترام .
عدم اتخاذ الإجراءات اللازمة لحماية البيانات: الإهمال .	تحمل مسؤولية حماية البيانات والمعلومات من الوصول: المسؤولية غير المصرح به.
استخدام البيانات بطرق تؤدي إلى التمييز ضد فئات: التمييز معينة من الأفراد.	ضمان المساواة في الوصول إلى المعلومات والخدمات، وعدم: العدل التمييز بين الأفراد.
إخفاء المعلومات المتعلقة بجمع البيانات أو استخدامها: التستر .	توفير معلومات واضحة وصادقة حول كيفية جمع البيانات: الشفافية واستخدامها.

"Google" التصدير إلى "جداول بيانات

- **مشاركة الجدول مع الزملاء:**
 - يمكن مشاركة الجدول في نقاش مع الزملاء، وتبادل الآراء حول أهمية القيم الأخلاقية في الأمن السيبراني.
 - يمكن أيضاً البحث عن أمثلة واقعية لممارسات الأمن السيبراني التي تتوافق مع القيم الأخلاقية أو تتعارض معها.