المحاضرة رقم 10: أمن المعلومات والمعاملات في التجارة الإلكترونية

الخطة العامة للمحاضرة

1. مقدمة
2. مفهوم أمن المعلومات
3. أهداف أمن المعلومات
4. أنواع التهديدات الإلكترونية
5. عناصر أمن التجارة الإلكترونية
6. أدوات وتقنيات الحماية الرقمية
7. التشريعات الجزائرية المتعلقة بالأمن السيبراني
8. التحديات الأمنية في البيئة الرقمية
9. توصيات لتعزيز الأمن الإلكتروني
10. خاتمة
11. الأعمال الموجهة

1. مقدمة

في عالم رقمي سريع التطور، أصبحت حماية المعلومات الحساسة والمعاملات الإلكترونية شرطًا أساسيًا لاستمرارية وموثوقية أنشطة التجارة الإلكترونية. وتتجسد الحاجة إلى أمن المعلومات في حماية البيانات، المعاملات، وسائل الدفع، والهوية الرقمية للأطراف المتعاملة.

2. مفهوم أمن المعلومات

أمن المعلومات هو:
"مجموعة من السياسات، الإجراءات، والتقنيات المستخدمة لحماية المعلومات الرقمية من الوصول غير المصرّح به، التعديل، الإتلاف أو الانتحال."

وهو أحد المكونات الأساسية لحوكمة التجارة الإلكترونية.

3. أهداف أمن المعلومات

- السرية :(Confidentiality) منع الوصول غير المصرح به إلى المعلومات
- السلامة :(Integrity) الحفاظ على دقة المعلومات وعدم التلاعب بها
- الإتاحة :(Availability) ضمان توفر المعلومات للمستخدمين الشرعيين
- المصداقية :(Authenticity) التأكد من هوية الأطراف المتعاملة

- عدم الإنكار :(Non-repudiation) إثبات تنفيذ العملية من الطرفين

4. أنواع التهديدات الإلكترونية

التهديد	الوصف
التصيّد الإلكتروني(Phishing)	رسائل احتيالية لسرقة بيانات المستخدمين
الاختراق(Hacking)	الدخول غير المشروع إلى الأنظمة
البرمجيات الخبيثة(Malware)	فيروسات وتروجان تؤثر على النظام
هجمات حجب الخدمة(DDoS)	إغراق الموقع بطلبات مزيفة لإيقافه
الاحتيال المالي	استغلال ثغرات الدفع الإلكتروني
انتحال الهوية	تقمّص شخصية مستخدم آخر

5. عناصر أمن التجارة الإلكترونية

- البنية التحتية الآمنة للموقع :استضافة مؤمنة، شهادات SSL
- وسائل دفع مؤمنة :تشفير بيانات البطاقات، OTP
- إدارة صلاحيات المستخدمين :حسابات شخصية محمية
- أنظمة النسخ الاحتياطي والاستعادة (Backup)
- سجلات تتبع العمليات (Logs)

6. أدوات وتقنيات الحماية الرقمية

الأداة/التقنية	الاستخدام
SSL/TLS	تشفير الاتصالات بين المتصفح والخادم
جدران الحماية(Firewalls)	مراقبة ومنع الدخول غير المصرّح به
مضادات الفيروسات	كشف وإزالة البرمجيات الخبيثة
المصادقة الثنائية(2FA)	حماية إضافية للحسابات
الشهادات الرقمية	التحقق من هوية الموقع أو المستخدم
Blockchain	حماية سجلات المعاملات بطريقة لامركزية

7. التشريعات الجزائرية المتعلقة بالأمن السيبراني

تشمل النصوص القانونية ذات العلاقة:

- القانون 18-05 المتعلق بالتجارة الإلكترونية (خاصة المواد 10 إلى 23)
- الأمر 20-03 المتعلق بالجرائم السيبرانية (سنة 2020)
- القانون 15-04 المتعلق بالتوقيع والتصديق الإلكتروني

- قانون حماية الحياة الخاصة عند معالجة البيانات الشخصية
- المرسوم التنفيذي المتعلق بسلطة ضبط الأمن السيبراني المنشأة سنة 2022

8. التحديات الأمنية في البيئة الرقمية الجزائرية

- ضعف الوعي الأمني لدى المستخدمين
- استخدام كلمات مرور ضعيفة أو مكررة
- محدودية مزودي الأمن السيبراني المحليين
- نقص التكوين في مجال الأمن الرقمي
- ضعف التبليغ عن الحوادث الأمنية
- مواقع غير محمية بشهادات أمان

9. توصيات لتعزيز الأمن الإلكتروني

- توعية المستخدمين بمخاطر التصيد والاحتيال
- استخدام كلمات مرور قوية وتغييرها دوريًا
- تفعيل المصادقة الثنائية في الحسابات
- التأكد من وجود شهادة SSL في المواقع المتعامَل معها
- تحديث البرمجيات والتطبيقات بانتظام
- الاستثمار في فرق أمن المعلومات داخل المؤسسات
- التعاون مع شركات تأمين إلكتروني (Cybersecurity firms)

10. خاتمة

أمن المعلومات والمعاملات ليس مجرد إجراء تقني، بل هو ضمان لاستمرار الثقة في التجارة الإلكترونية. لذا، على المؤسسات الجزائرية والطلبة الجامعيين أن يولوا هذا الجانب أهمية كبيرة سواء من خلال التعلم أو الممارسة أو التوعية.

الأعمال الموجهة رقم 10(TD 10)

الموضوع :تحليل مخاطر الأمن الرقمي في التجارة الإلكترونية

المدة 90 :دقيقة

التمرين الأول: اختبار اختراق نظري(Threat Simulation)

الوضعية:

أنت مدير متجر إلكتروني يتعرض لمحاولة اختراق عبر هجمة تصيّد.(Phishing)

◀كيف تكتشف الهجمة؟ ما الخطوات الاستباقية والوقائية التي تتخذها؟

التمرين الثاني: تحليل موقع إلكتروني

المهمة:

قم باختيار موقع جزائري للتجارة الإلكترونية) مثلاًJumia.dz :، (...Ouedkniss، ثم:

- تحقق من وجود شهادة SSL
- افحص طريقة تسجيل الدخول (كلمة مرور– مصادقة ثنائية...)
- حدّد المخاطر المحتملة التي يواجهها الموقع
- قدّم توصيات لتحسين أمانه

التمرين الثالث: جدول تحليل تهديدات

أكمل الجدول التالي:

التهديد	مصدره المحتمل	التأثير على المؤسسة	الحل التقني المناسب
Phishing			
Malware			
DDoS			

المراجع المعتمدة

1. Stallings, W. (2022). *Cryptography and Network Security*. Pearson.
2. Laudon, K. C., & Traver, C. G. (2023). *E-Commerce: Business, Technology, Society*.
3. ENISA (2024). *Cybersecurity Guidelines for SMEs*.
4. مركز الأمن السيبراني الجزائري (CSA)
5. قانون 18-05 + الأمر 20-03 (الجرائم السيبرانية)
6. OWASP Top 10 Threats Report (2025)