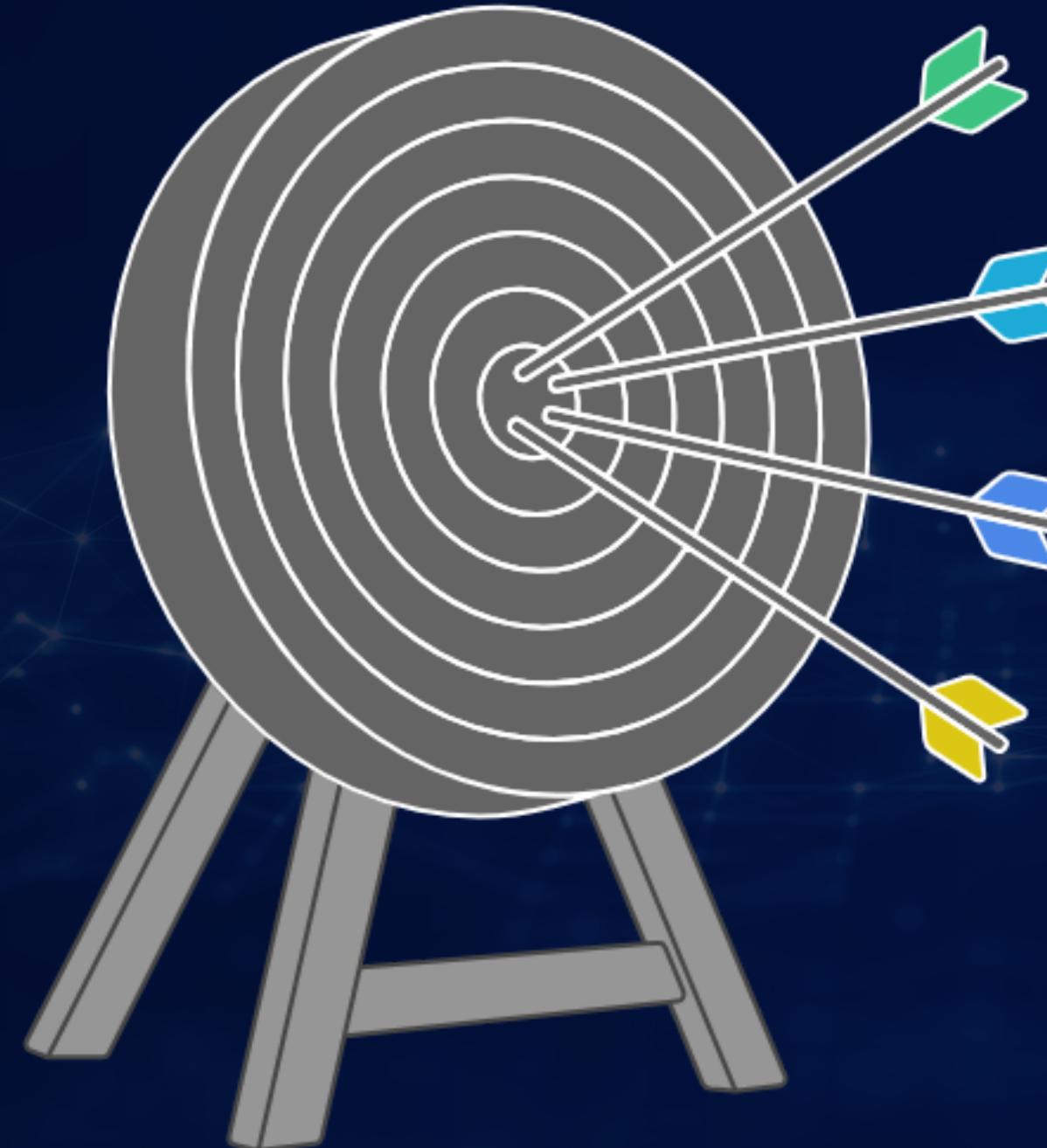




الدرس الشانسي

CYBER SECURITY

يتناول الدرس الثاني مجموعة من العناصر



ممارسات أمان يومية
واستجابة للحوادث



أمن الشبكات الأساسية



المصادقة وإدارة الهوية



أنواع التهديدات والهجمات
السيبرانية

أنواع التهديدات والهجمات السيبرانية (Threats & Attack Vectors)

أنواع التهديدات السيبرانية

ثغرات التطبيقات



البرمجيات الخبيثة



الهجمات على الشبكة

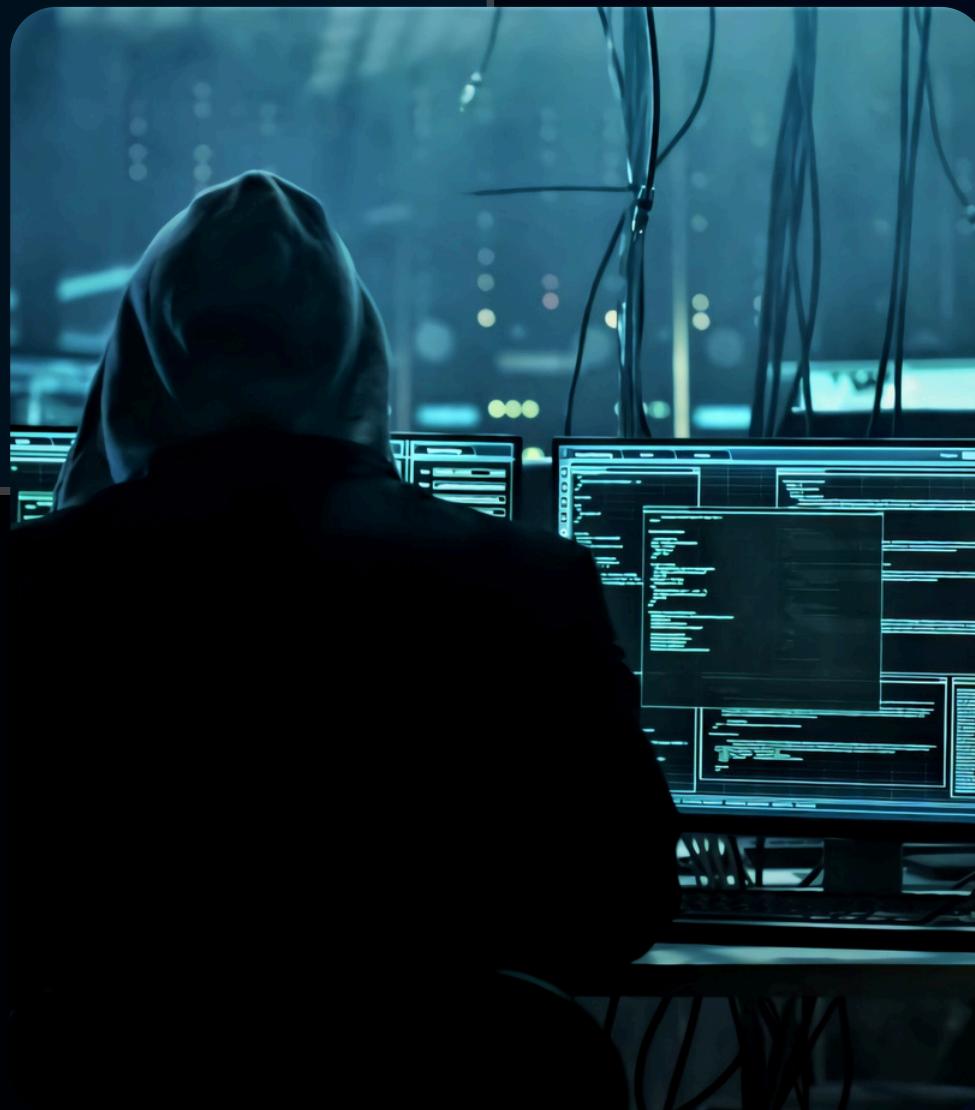


التصيد



الهندسة الاجتماعية

أنواع التهديدات والهجمات السيبرانية (Threats & Attack Vectors)

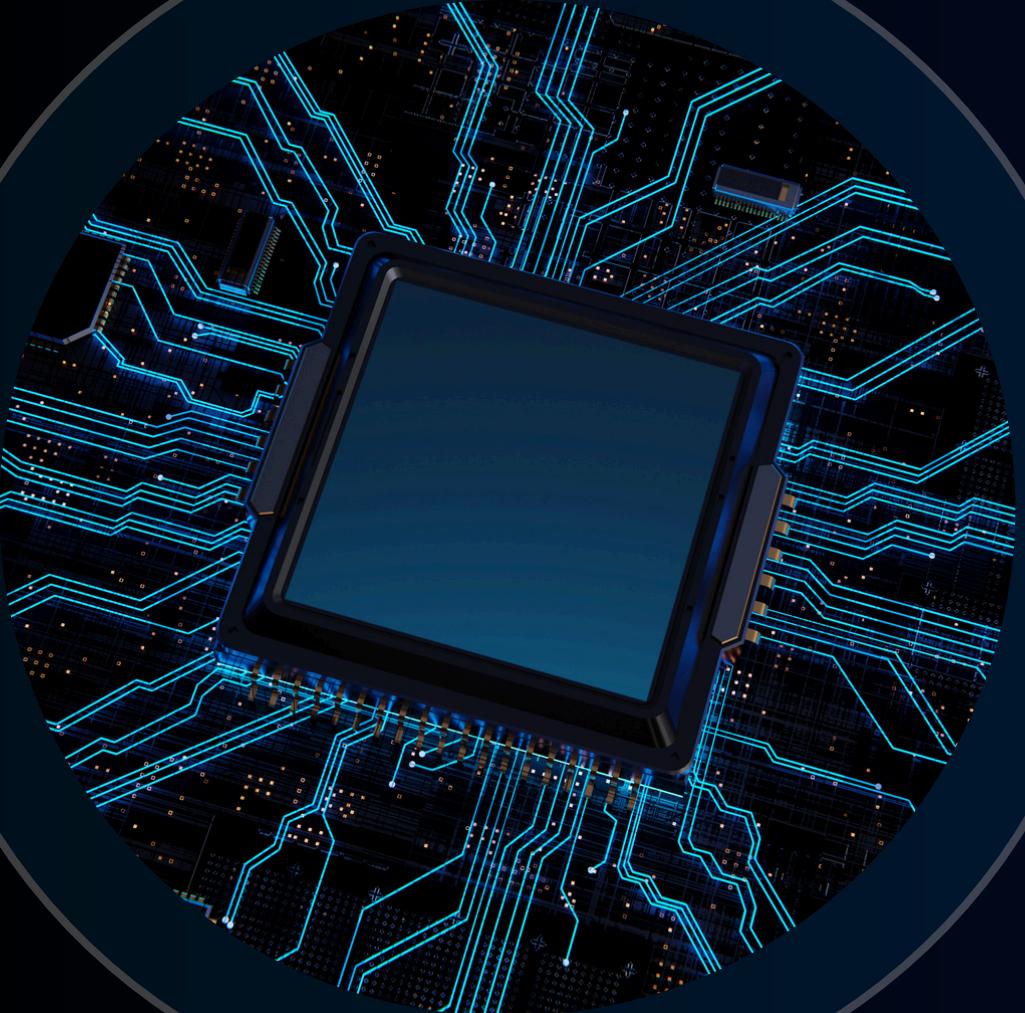


البرمجيات الخبيثة (MALWARE)

1

برنامج أو ملف مصمم لإلحاق ضرر، مثل الفيروسات، الديдан، وبرامج الفدية (Ransomware). نشره يحدث عبر مرافق بريدية، تنزيلات مشبوهة أو ثغرات نظامية

أنواع التهديدات والهجمات السيبرانية (Threats & Attack Vectors)

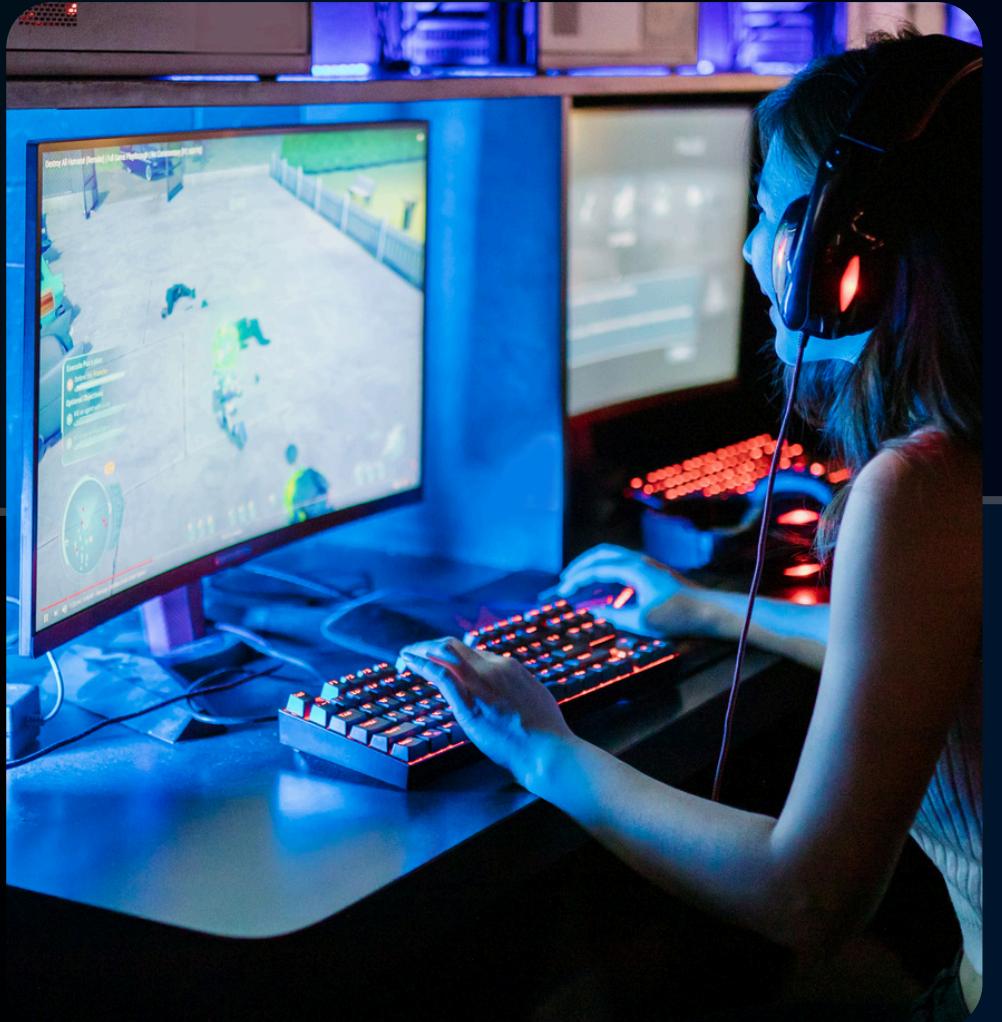


التصيد (Phishing)

2

سأئل أو صفحات مزيفة تهدف لاستخراج
بيانات دخول أو معلومات شخصية عن
طريق خداع المستخدم.

أنواع التهديدات والهجمات السيبرانية (Threats & Attack Vectors)



الهندسة الاجتماعية (Social Engineering)

3

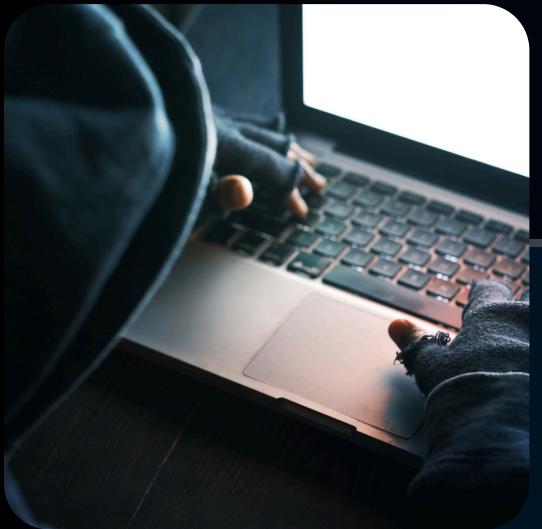
استغلال الثقة أو الجهل البشري (مثلاً:
مكالمات تطلب إعادة تعيين كلمة
المرور).

أنواع التهديدات والهجمات السيبرانية (Threats & Attack Vectors)

4

الهجمات على الشبكة (مثل DDoS)

إغراق الخدمة بطلبات تجعلها غير متاحة
للمستخدمين الشرعيين



أنواع التهديدات والهجمات السيكரانية (Threats & Attack Vectors)

5 ثغرات التطبيقات والبنية التحتية

استغلال أخطاء برمجية أو إعدادات خاطئة للوصول غير المصرح أو للسيطرة على أنظمة.



أمثلة تطبيقية مناسبة لطلاب تكنولوجيا التعليم



رسالة تصيد تبدو كطلب من منصة
ادارة التعليم (LMS) لإدخال بيانات
اعتماد.

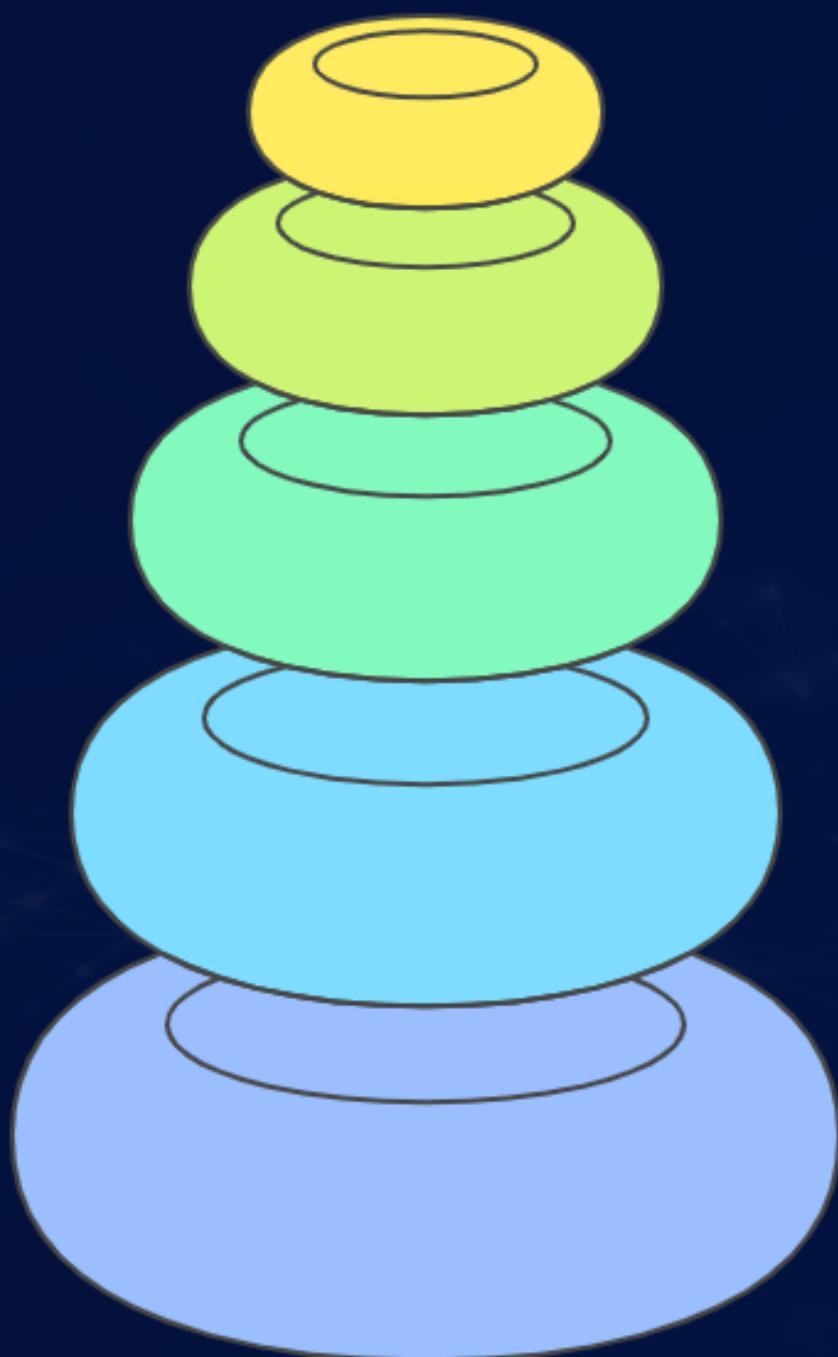


ملف اختبار يحتوي على كود
يحاول نشر نفسه عند فتحه.



المصادقة وإدارة الهوية Authentication & (Access Control)

المصادقة وإدارة الهوية (Authentication & Access Control)



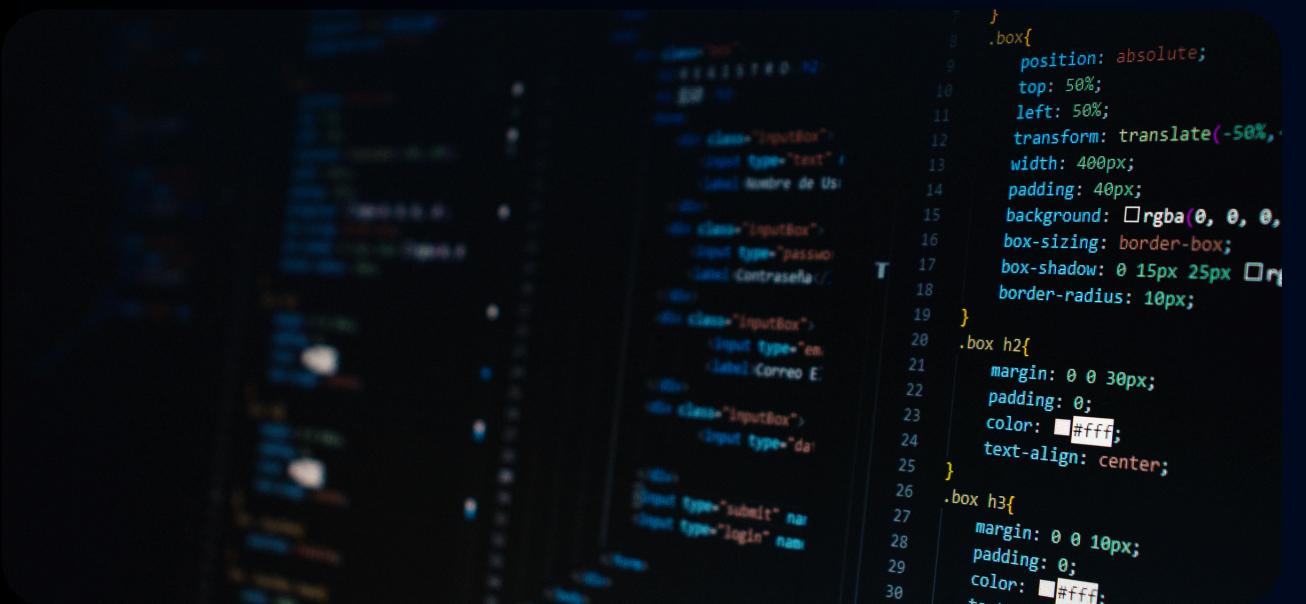
- دورات الصلاحية Authentication & Access Control
- مبدأ أقل الامتيازات Least Privilege
- المصادقة متعددة العوامل Multi-factor Authentication
- مدير كلمات المرور Password Manager
- كلمات المرور القوية Strong Passwords

المصادقة وإدارة الهوية (& Access Control)

1

كلمات المرور القوية

طول مناسب، مزيج أحرف/أرقام/
رموز، تجنب إعادة الاستخدام.



2

المصادقة متعددة العوامل (MFA)
رمز مؤقت، تطبيق) إضافة طبقة
تقلل مخاطر (SMS مصادقة، رسالة
سرقة الحساب حتى لو خُرِقت كلمة
المرور.



أمن الشبكات الأساسية

Network Security) Basics



أُمن الشبكات الأساسية (Network Security Basics)

1

شبكات Wi-Fi آمنة

تغيير اسم الشبكة الافتراضي، استخدام تشفير قوي (WPA2/WPA3).
إخفاء إعدادات الإدارة.

2

الشبكات الضيف (Guest)
فصل شبكة الضيوف عن شبكة الأجهزة
الحسامة للمؤسسة التعليمية.



3

استخدام VPN
عند الاتصال من شبكات عامة لتشفيه الاتصال
وحماية نقل البيانات.

أُمن الشبكات الأساسية (Network Security Basics)

4

جدران الحماية (Firewall)

وإدارة الأجهزة المتصلة: فهم بسيط
لكيفية حجب منافذ غير ضرورية
ومراقبة الأجهزة المتصلة بالشبكة.



تأمين نقاط الوصول في الفصول الذكية
للأجهزة الذكية تحديث firmware
وتغيير كلمات المرور الافتراضية.

5



ممارسات أمان يومية واستجابة للحوادث

Good Practices & (Incident Response)



ممارسات أمان يومية واستجابة للحوادث (Good Practices & Incident Response)

التحديث والنسخ الاحتياطي

أهمية تثبيت تحديثات النظام والبرامج فور توفرها، وأهمية نسخ البيانات المهمة (نسخ محلية وآمنة وسحابة).



سياسات استخدام الأجهزة

قواعد واضحة لاستخدام الأجهزة الشخصية

والمنصات داخل البيئة التعليمية (مثل عدم

تثبيت برمجيات غير مرخصة)

مراقبة وأبلاغ الحادث

تعريف ما هو الحادث الأمني، قنوات الإبلاغ، المعلومات

المطلوبة عند الإبلاغ (متى، ماذا، من تواصل معه).



1

2

3

ممارسات أمان يومية واستجابة للحوادث (Good Practices & Incident Response)

خطة استعادة بسيطة

4

خطوات فصل جهاز مصاب، حفظ السجلات، إعادة تعيين كلمات المرور، واستعادة النسخ الاحتياطية.



التوعية المستمرة

حملات توعية قصيرة ومستمرة للطلاب وأعضاء هيئة التدريس.

5

