ملخص الوحدة 3: أمن المعلومات

البرمجة والذكاء الاصطناعي، أولى ثانوي

مهندس رحيم

3-1 تهديدات وإجراءات مواجهة أمن المعلومات (1)

- **يعني إيه أمن المعلومات؟**
  - **السرية (Confidentiality):** اللي مسموح لهم بس هم اللي يوصلوا للمعلومة.
  - **السلامة (Integrity):** المعلومة ما اتدمّرتش ولا حد عبث بيها ولا اتمسحت.
  - **التوافرية (Availability):** المعلومة موجودة وتقدر توصلها في أي وقت تحتاجها.
- **إزاي تعرف العنصر اللي اتضرب؟**
  - موقع وقع بسبب هجوم إلكتروني ← اتضربت **التوافرية**.
  - بيانات غلط اتكتبت أو اتعدلت ← اتضربت **السلامة**.
  - بيانات شخصية اتسربت أو حد غريب شافها ← اتضربت **السرية**.
- **الوصول غير المصرّح به والاختراق: الوصول غير المصرّح به (Unauthorized access):** حد ملوش صلاحية يدخل على نظام كمبيوتر.
- **البرمجيات الخبيثة (Malware)**
  - **فيروس الكمبيوتر (Computer virus):** يدمّر بيانات أو برامج عن قصد.
  - **حصان طروادة (Trojan horse):** يتنكر في شكل برنامج سليم
  - **الدودة (Worm):** تنسخ نفسها وتنتشر على الإنترنت لوحدها
  - **برنامج التجسس (Spyware):** يجمع بياناتك الشخصية من غير علمك ويبعتها لطرف تالت
  - **برنامج الفدية (Ransomware):** يقفل بياناتك ويطلب فلوس (فدية) عشان يرجّعهالك.
- **الجريمة الإلكترونية (Cybercrime)**
  - **انتهاك قانون الوصول غير المصرّح به للكمبيوتر:** تدخل على كمبيوتر باسم مستخدم وكلمة مرور بتوع حد تاني
  - **جرائم الكمبيوتر والسجلات الإلكترونية:** العبث بالبيانات المخزنة أو التلاعب بالأجهزة من غير تصريح.
  - **جرائم قائمة على الشبكة:** نصب أو تشهير أو انتهاك حقوق المؤلف عن طريق الشبكة.
- **هجمات حجب الخدمة (DoS و DDoS): هجوم حجب الخدمة (DoS - Denial of Service):** المهاجم بيغرّق السيرفر بكمية طلبات ضخمة من **جهاز واحد**

Information security	أمن المعلومات: إدارة المعلومات صح والحفاظ عليها آمنة
Confidentiality	السرية: المصرّح لهم بس يوصلوا للمعلومة
Integrity	السلامة: المعلومة ما اتدمرتش ولا اتعدلت ولا اتمسحت
Availability	التوافرية: المعلومة متاحة وقت الحاجة
Cracking	الاختراق: دخول غير قانوني للعبث بالبيانات أو سرقتها
Malware	البرمجيات الخبيثة: اسم عام للبرامج الضارة
Trojan horse	حصان طروادة: برنامج متنكر كبرنامج سليم ويهاجم في هدوء
Worm	الدودة: برنامج ينسخ نفسه وينتشر على الإنترنت
Spyware	برنامج التجسس: يجمع بياناتك من غير علمك ويبعتها لغيرك
Ransomware	برنامج الفدية: يقفل البيانات ويطلب فدية
DoS attack	هجوم حجب الخدمة: إغراق السيرفر بطلبات من جهاز واحد لحد ما يقع
DDoS attack	هجوم حجب الخدمة الموزّع: إغراق السيرفر بطلبات من أجهزة كتير مع بعض

3-2 التهديدات والتدابير المضادة في أمن المعلومات (2)

- **كلمة المرور (Password)**
  - خليها **طويلة** على قد ما تقدر.
  - **اخلط:** حروف كبيرة وصغيرة وأرقام ورموز.
  - ما تستخدمش بياناتك الشخصية (عيد ميلادك
  - ما تكررش نفس كلمة المرور في أكتر من خدمة
- **احسبها: كام تركيبة ممكنة؟**: لو عندك **n** رمز مسموح وطول كلمة المرور **k**
- **المصادقة (Authentication) وأنواعها**
  - **المصادقة القائمة على المعرفة (Knowledge-based):** حاجة إنت بس اللي تعرفها
  - **المصادقة البيومترية (Biometrics):** صفة في جسمك أو سلوكك
  - **المصادقة القائمة على الحيازة (Possession-based):** حاجة معاك
- **ثنائية ولا متعددة الخطوات؟**
  - **المصادقة الثنائية (Two-factor):** عاملين من **نوعين مختلفين** (مثلًا PIN + كود SMS = معرفة + حيازة).
  - **المصادقة متعددة الخطوات (Two-step):** خطوتين بمعلومتين من **نفس النوع** (مثلًا كلمة مرور + سؤال سري
  - **كلمة المرور لمرة واحدة (One-time password):** بتتغير كل فترة وتنفع مرة واحدة بس
- **إجراءات أمن المعلومات**
  - **التحكم في الوصول (Access control):** نحدد مين بس يستخدم النظام أو البيانات
  - **جدار الحماية (Firewall):** عند مدخل الشبكة؛ يمنع **الوصول غير المصرح به** من بره و**تسرّب البيانات** من جوه.
  - **ضد الفيروسات:** ثبّت **برنامج مكافحة الفيروسات** وحدّث تعريفاته
- **مبدأ أقل الصلاحيات (Least Privilege)**: جزء من **التحكم في الوصول**: كل مستخدم ياخد **أقل صلاحيات** يحتاجها علشان يعمل شغله

Password	كلمة المرور: حروف تثبت إنك صاحب الحساب
One-time password	كلمة المرور لمرة واحدة: بتتغير كل فترة وتنفع مرة واحدة
Authentication	المصادقة: التحقق من هوية المستخدم
Biometric authentication	المصادقة البيومترية: بصمة، قزحية، وريد، خط يد
Possession-based authentication	المصادقة القائمة على الحيازة: حاجة معاك زي بطاقة أو كود SMS
Two-factor authentication	المصادقة الثنائية: عاملين من نوعين مختلفين
Two-step authentication	المصادقة متعددة الخطوات: خطوتين من نفس النوع
Access control	التحكم في الوصول: قصر الاستخدام على مستخدمين محددين
Firewall	جدار الحماية: يمنع الدخول من بره وتسرب البيانات من جوه
Security hole	الثغرة الأمنية: نقطة ضعف في البرنامج بتتقفل بالتحديث
Least privilege	أقل الصلاحيات: كل مستخدم ياخد أقل صلاحيات يحتاجها لشغله

3-3 التهديدات والتدابير المضادة في أمن المعلومات (3)

- **الاحتيال بالفواتير**
  - **فاتورة احتيالية (Fraudulent billing):** يبعتولك فاتورة لخدمة وهمية عمرك ما استخدمتها
  - **الاحتيال بنقرة واحدة (One-click fraud):** تدوس على رابط في موقع أو إيميل
- **التصيّد (Phishing)**: موقع **مزيف** متنكر في شكل بنك أو جهة رسمية
- **الهندسة الاجتماعية (Social engineering)**
  - **انتحال الشخصية (Impersonation):** يكلمك على إنه شخص تاني (موظف
  - **التجسس المباشر (Shoulder surfing):** يبص من ورا كتفك على الشاشة أو الكيبورد وإنت بتكتب كلمة المرور أو الـ PIN.

- **البحث في المهملات (Dumpster diving):** يدوّر في الزبالة على ورق سري اترمى.
- **التزوير (Skimming)**: سحب بيانات **بطاقة الائتمان أو الخصم** بتاعة حد بشكل غير قانوني
- **سياسة أمن المعلومات (Information Security Policy)**
  - **السياسة الأساسية:** المبادئ والإعلان العام للمنظمة عن أمن المعلومات.
  - **معايير الأمان:** القواعد اللي بتطبّق السياسة الأساسية عمليًا.
  - **إجراءات التنفيذ وقواعد التشغيل:** خطوات واضحة حسب الفئة المستهدفة والغرض.
- **سياسة الاستخدام الآمن (Acceptable Use Policy)**
  - ما تدّيش حسابك أو كلمة المرور لحد
  - ما تنشرش محتوى مسيء أو ضار
  - استخدم الأجهزة والشبكة للغرض اللي اتعملت علشانه (الدراسة مثلًا).
  - إنت **مسؤول** عن اللي بيتعمل بحسابك؛ مخالفة السياسة ليها عقوبات زي إيقاف الحساب

Fraudulent billing	فاتورة احتيالية: فاتورة لخدمة وهمية ما استخدمتهاش
One-click fraud	الاحتيال بنقرة واحدة: نقرة على رابط تطلع عقد وهمي وطلب دفع
Phishing	التصيّد: موقع مزيف كبنك أو جهة رسمية لسرقة البيانات
Social engineering	الهندسة الاجتماعية: استغلال نفسية الإنسان وإهماله
Impersonation	انتحال الشخصية: التظاهر بإنك شخص تاني
Shoulder surfing	التجسس المباشر: البص على الشاشة أو الكيبورد وقت كتابة كلمة المرور
Dumpster diving	البحث في المهملات: التدوير في الزبالة على معلومات سرية
Skimming	التزوير: سحب بيانات الكارت لعمل كارت مزور
Information security policy	سياسة أمن المعلومات: قواعد المنظمة الأساسية لحماية المعلومات
Acceptable use policy	سياسة الاستخدام الآمن: قواعد المسموح والممنوع عند استخدام أجهزة وحسابات جهة معينة

3-4 تقنيات المعلومات للسلامة (1)

- **مصطلحات التشفير**
  - **التشفير (Encryption):** نحوّل الرسالة وقت الإرسال عشان محدش غير المستلم المقصود يفهمها لو اعترضها.
  - **النص العادي (plaintext):** الرسالة الأصلية قبل التشفير
  - **فك التشفير (Decryption):** نرجّع النص المشفر لنص عادي.
  - **المفتاح (Key):** الإجراء أو البيانات اللي بنشفّر ونفك بيها.
- **التشفير بالمفتاح المتماثل (Symmetric key): نفس المفتاح:**
- **التشفير بالمفتاح العام (Public key):** مفتاحين: **المفتاح العام (public key)** متاح لأي حد
- **مقارنة**
  - **المتماثل:** أسرع في التشفير وفك التشفير
  - **العام:** إدارة المفاتيح أسهل لأن المفتاح العام بيتوزع بحرية
- **طريقة المفتاح المؤقت (Session key method):** بتجمع النوعين: **التشفير بالمفتاح العام** لتوصيل المفتاح المشترك بأمان

Encryption	التشفير: منع غير المستلم من فهم الرسالة
Plaintext	النص العادي: الرسالة الأصلية قبل التشفير
Ciphertext	النص المشفر: الرسالة بعد التشفير
Decryption	فك التشفير: رجوع النص المشفر لنص عادي
Key	المفتاح: الإجراء أو البيانات المستخدمة للتشفير وفكه
Symmetric key encryption	التشفير بالمفتاح المتماثل: نفس المفتاح للتشفير وفكه

Shared key	المفتاح المشترك: المفتاح الواحد عند الطرفين
Public key encryption	التشفير بالمفتاح العام: نشفّر بالعام ونفك بالخاص
Private key	المفتاح الخاص: مع المستلم بس ويفك بيه
Session key method	طريقة المفتاح المؤقت: تجمع التشفير المتماثل والعام

3-5 تقنيات المعلومات للسلامة (2)

- **دالة التجزئة (Hash function)**
  - نفس البيانات + نفس الدالة ← **دايمًا نفس القيمة**.
  - تغيير حرف واحد ← قيمة **مختلفة تمامًا** (مش حرف واحد بس).
  - **مش ممكن:** ترجّع البيانات الأصلية من قيمة التجزئة.
- **التوقيع الرقمي (Digital signature)**: تقنية بتستخدم **التشفير بالمفتاح العام + قيم التجزئة** عشان تثبت إن البيانات **جاية من المرسل فعلًا** و**محدش عبث بيها**
- **الخطوات بالترتيب**
  - **المرسل 1:** يطلّع قيمة التجزئة من النص العادي بدالة التجزئة.
  - **المرسل 2:** يشفّر قيمة التجزئة بـ **المفتاح الخاص للمرسل** ← ده هو **التوقيع الرقمي**.
  - **المرسل 3:** يبعت النص العادي + التوقيع الرقمي.
  - **المستلم 4:** يفك التوقيع بـ **المفتاح العام للمرسل** ويطلّع قيمة التجزئة الأصلية.
  - **المستلم 5:** يطلّع قيمة تجزئة جديدة من النص اللي وصله بنفس الدالة.
  - **المستلم 6:** يقارن القيمتين: **لو متطابقين** ← الرسالة من المرسل وما اتعدلتش.
- **جهة التصديق (CA)**: التوقيع لوحده ما يمنعش **انتحال الشخصية**: ممكن حد يدّعي إن مفتاح عام معيّن بتاعه
- **SSL/TLS و https: SSL/TLS**: بيشفّر الاتصال بين **خادم الويب** و**متصفح الويب** بـ **طريقة مفتاح الجلسة (Session key)**

Hash function	دالة التجزئة: تحسب قيمة فريدة من البيانات
Hash value	قيمة التجزئة: ناتج دالة التجزئة، وما ترجعش للأصل
Digital signature	التوقيع الرقمي: يثبت المرسل وإن البيانات ما اتعدلتش
Certification authority (CA)	جهة التصديق: طرف تالت موثوق يصدر الشهادات الرقمية
Digital certificate	الشهادة الرقمية: فيها المفتاح العام وبيانات صاحبه
SSL/TLS	تشفير الاتصال بين المتصفح وخادم الويب
HTTPS	بداية رابط الصفحة المشفرة بـ SSL/TLS

ذاكر المادة كلها مجاناً

شرح كل الدروس، أسئلة بالإجابات، بنك على نمط الوزارة، وامتحان بشكل الوزارة

zerooneacademy.com

مهندس رحيم