المحور الثالث: الأمن المعلوماتي

Information security (InfoSec)

د. سفيان خلوفي

مفهوم الأمن المعلوماتي

تهديدات أمن المعلومات

طرق مواجهة تهديدات أمن المعلومات

الأمن السيبراني

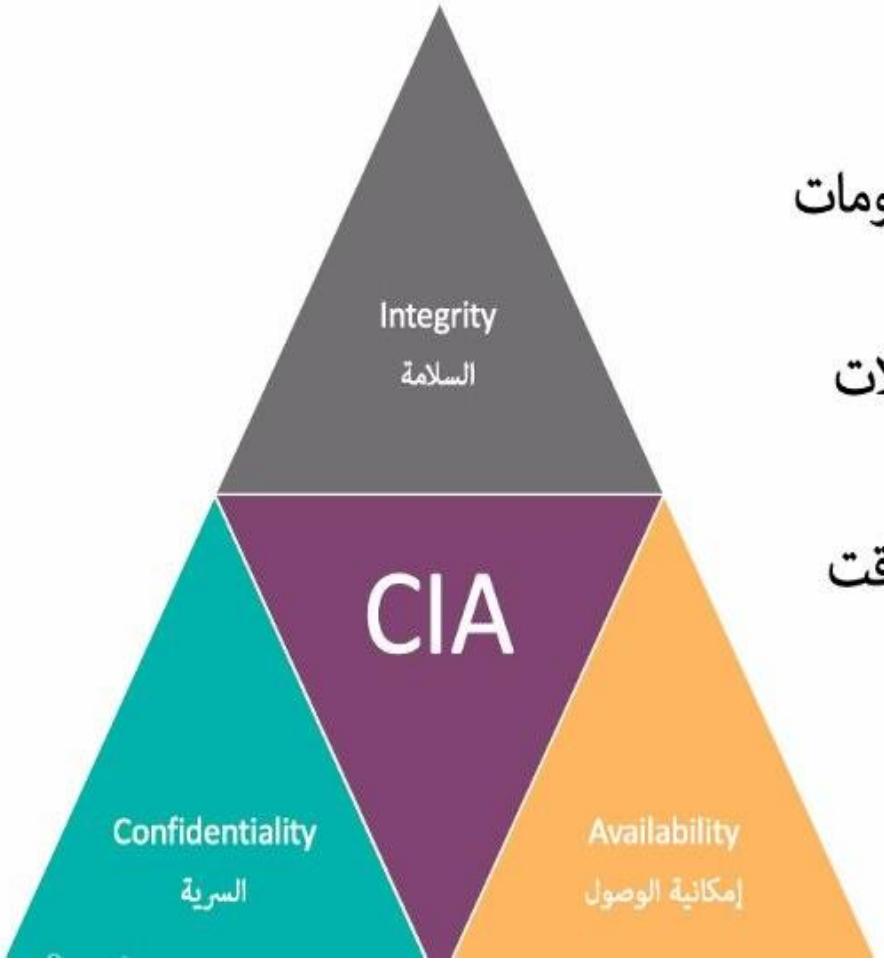
مفهوم الأمن المعلوماتي

مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية

المعلومات من الوصول غير المصرح به، أو الاستخدام غير

المصرح به، أو الكشف، أو التعطيل، أو التعديل، أو التدمير.

ويقوم أمن المعلومات على ثلاثة أبعاد رئيسية، يشار إليها غالبًا باسم– **ثلاثية CIA Triad:**



- **السرية Confidentiality**

عدم إمكانية الوصول الغير مصرح به للبيانات او المعلومات

- **السلامة Integrity**

حماية البيانات أو المعلومات من أي تغييرات أو تعديلات

- **إمكانية الوصول Availability**

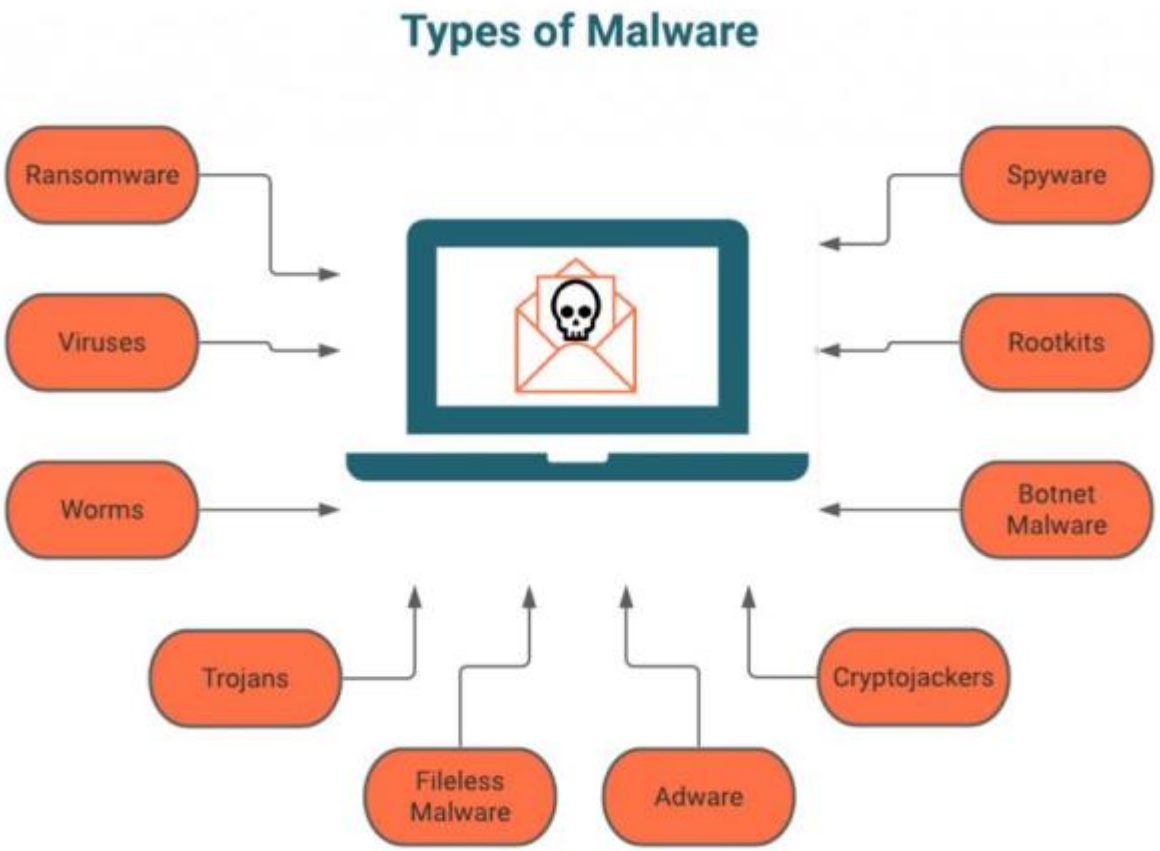
امكانية الوصول للبيانات من قبل المصرح له وفي أي وقت

تهديدات أمن المعلومات

1- البرمجيات الخبيثة (Malware):

وتشمل الفيروسات، والديدان، وأحصنة طروادة، وبرامج التجسس، وبرامج الفدية، وغيرها، وتهدف إلى السيطرة على الجهاز وتمكين المخترقين من الوصول إلى المعلومات بسهولة، أو تدمير الجهاز وإتلاف محتوياته وملفاته وبرامج تشغيله.

أهداف البرمجيات الخبيثة:



التسبب في أضرار

سرقة معلومات

تعطيل الأنظمة

التجسس

الفيروس Virus

برنامج ضار ينسخ نفسه ويصيب الملفات الأخرى.

Virus

هو عبارة عن ملف ضار هدفه تخريبي , يحتاج للتشغيل النظام لكي يعمل , وينتقل من نظام لاخر

الاعراض

بطئ في الأداء
ظهور رسائل غريبة في النظام
تعطيل البرامج

الديدان Worms

برامج صغيرة قائمة بذاتها غير معتمدة على غيرها صنعت للقيام بأعمال تدميرية أو لغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم للإنترنت أو إلحاق الضرر بهم أو بالمتصلين بهم، تمتاز بسرعة الانتشار ويصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة

برامج التجسس Spyware

هي برامج حاسوبية تُثبت خلسةً على أجهزة الحاسوب للتجسس على المستخدمين أو للسيطرة جزئيًا على الحاسوب الشخصي، من دون علم المستخدم

برنامج الفدية Ransomware

يحتجز بيانات الضحية ويطلب فدية لفك التشفير.

Ransomware

وهو من اشهر أنواع الملفات الضارة الحالية , و هدفه مادي , وليس تعطيل و ليس تعطيل و تخريب فقط ,فهي برامج تشفر البيانات و تطلب فدية مالية لفك تشفير النظام

الاعراض

قفل النضام او ملفات النضام
رسائل تطلب بفدية لفك التشفير

حصان طروادة Trojan Horse

برنامج يبدو شرعياً لكنه يحمل برمجيات ضارة.

Trojan Horse

هو برنامج ضار يبدو بصورة مشروعة او مفيدة , و لمنها تحتوي على تعليمات و برامج خبيثة , وهدفه سرقة البيانات و تخميل برامج ضارة أخرى , التجسس

الاعراض

تغييرات في النظام بدون مبرر
تحميل برامج غير معروفة تلقائنا

الإعلانات الضارة Adware

نوع من البرامج الخبيثة التي تُثبّت نفسها سرًا على جهازك وتعرض إعلانات ونوافذ منبثقة غير مرغوب فيها. في بعض الحالات، يمكن لبرامج الإعلانات الضارة تتبع سلوكك على الإنترنت وعرض إعلانات مخصصة.

مسجل المفاتيح Keylogger

يسجل ضغطات المفاتيح لسرقة كلمات المرور والمعلومات.

Keyloger

برمجيات مصصمة لجمع المعلومات من النظام دون علم المستخدم , من أهدافها تسجيل ضغطات المفاتيح , سرقة معلومات تسجيل الدخول , جمع البيانات الشخصية

الاعراض

بطئ غير مبرر
ظهور إعلانات غير مرغوب فيها
تغييرات في اعدادات و اذونات النظام

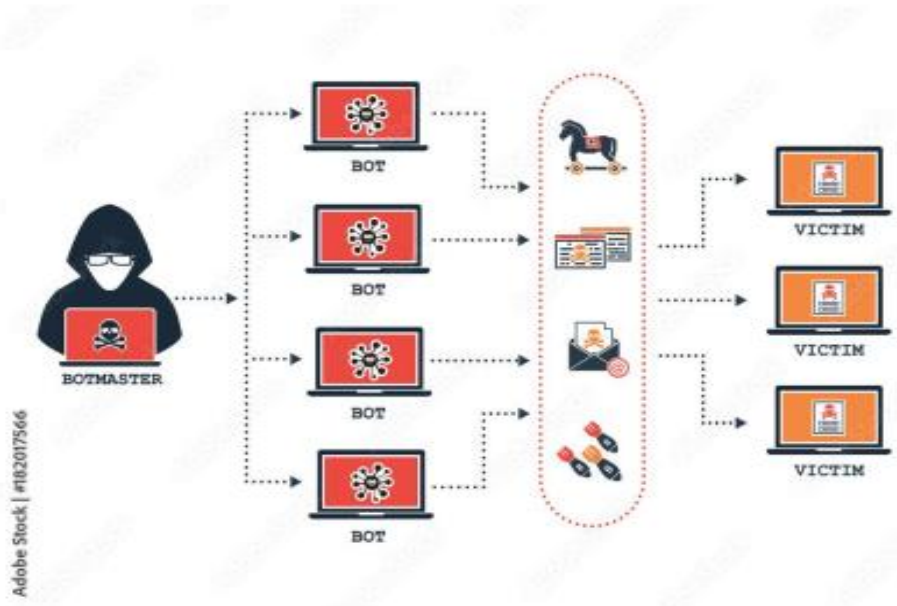
https://youtu.be/9HCmuaertF8

البوتات وشبكات البوت Bots and Botnet

تستخدم أجهزة مصابة للتحكم عن بُعد وشن هجمات

Bots and Botnet

شبكات من الأجهزة المخترقة تستخدم لتنفيذ هجمات كبيرة على نضام معين



الاعراض

استخدام غير طبيعي للمواد
بطئ في الأداء للنظام و كذلك الشبكة

2. التصيد الاحتيالي (Phishing)

وهو محاولة للحصول على معلومات حساسة عن طريق انتحال شخصية جهة موثوقة.

هذا النوع من التهديدات يُعرف أيضًا بـ **"انتحال الهوية الرقمية لمؤسسة "**يهدف في الغالب **للاحتيال المالي.** وهو من أشكال **الهندسة الاجتماعية على الشركات.**

Social Engineering

هي فن التلاعب بالمستخدمين من اجل خداعهم و اقناعهم بالقيام لاعمال تؤدي لكشف بياناتهم و او حساباتهم السرية بدون علمهم

أسباب نجاح الهندسة الاجتماعية على الشركات

عدم وجود تدريب امني كافي للموضفين

عدم التنظيم في الدخول الى بيانات الشركة

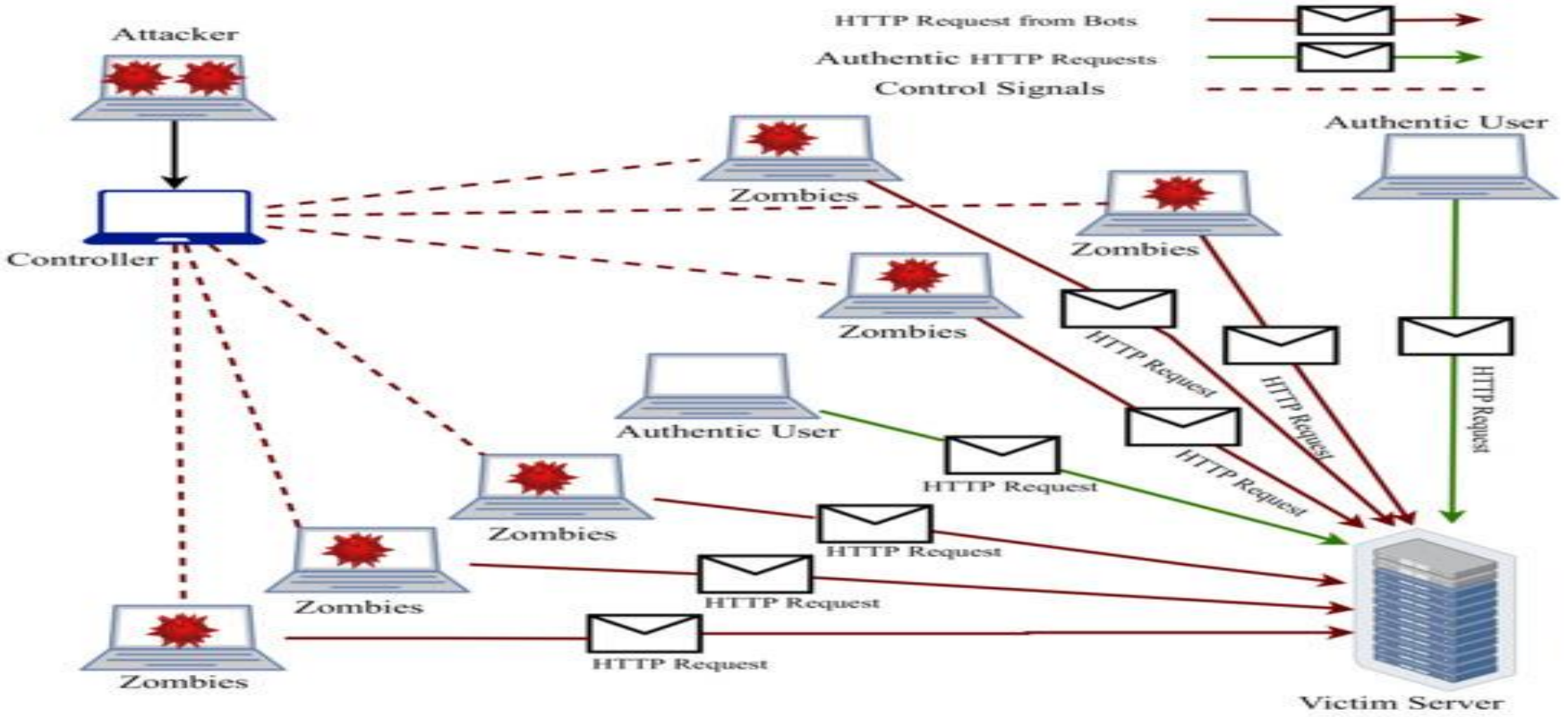
اعطاء للموضفين صلاحية حساسة

صعوبة التعرف على حالة الهندسة الاجتماعية و التفرقة بينها و بين الحقيقة

لا توجد برامج لحماية من الهندسة الاجتماعية

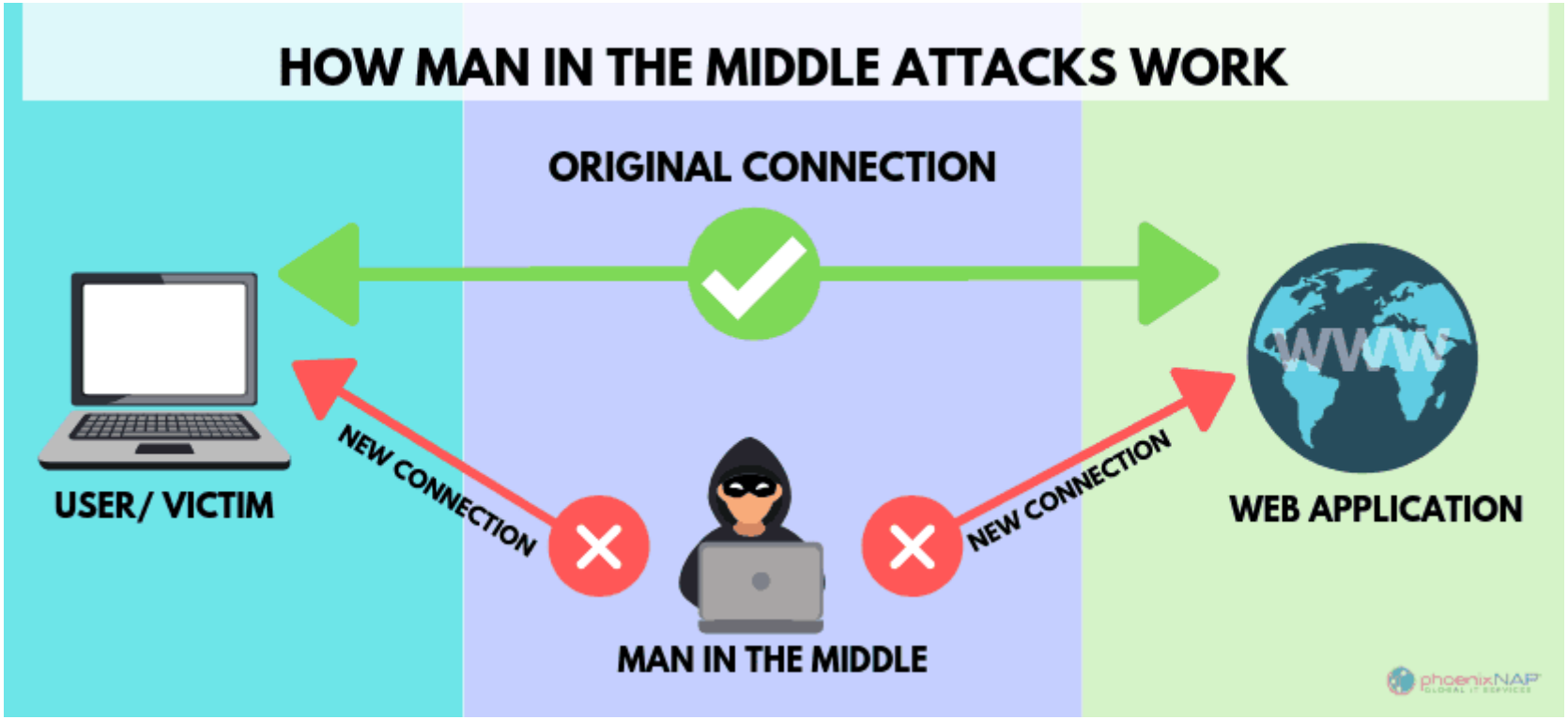
3. هجمات الحرمان من الخدمة (Denial-of-Service Attacks)

تهدف إلى تعطيل عمل نظام أو شبكة عن طريق إغراقها بكميات كبيرة من حركة المرور.



4. هجمات الوسيط
(Man-in-the-Middle Attacks)

وفيها يقوم المهاجم باعتراض الاتصال بين طرفين وتبادل المعلومات بينهما دون علمهما.



5. التهديدات الداخلية (Insider Threats)

وتشمل التهديدات التي تأتي من داخل المؤسسة، سواء من قبل موظفين حاليين أو سابقين.

6. الاختراق الأمني

هو عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر وتصريحات الدخول بهدف الاطلاع على المعلومات، أو تخريبها، أو سرقتها.

الاختراق يرتبط بالدخول غير المشروع إلى أمور محمية بالأمان

ترتبط الهجمات الإلكترونية بالاستخدام الخبيث للتكنولوجيا لتسبب الضرر

https://www.youtube.com/watch?v=rR1F_R_7HDk

7. الاحتيال المالي:

يتضمن الاحتيال واستعمال أجهزة الصرف الآلي، وبطاقات وحسابات مزورة وسرقة البيانات وسرقة بطاقات الائتمان، ويتضمن أيضًا الجرائم الناتجة عن السرقات والتعديات المالية على حسابات البنوك ومراكز التعامل المالي من خلال اختراق أنظمتها وتحويل الحسابات والأرصدة للمخترقين.

8. غسيل الأموال

عملية تحويل الأموال المتحصلة من أنشطة إجرامية بهدف إخفاء أو إنكار المصدر غير الشرعي والمحظور لهذه الأموال أو مساعدة شخص ارتكب جرمًا ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم.

9. الكوارث

الحوادث التي تؤثر على نظم المعلومات، وتنقسم إلى **كوارث طبيعية** مثل الزلازل والأعاصير والفيضانات والحرائق، وكوارث ناتجة عن **أسباب تقنية** كانقطاع التيار الكهربائي، أو حدوث عطل في أحد أجهزة الحاسب الآلي أو برمجياته، بالإضافة إلى **الأعمال التخريبية** التي تشمل جميع الأعمال التي تؤدي إلى تعطل الجهاز بشكل متعمد، وتدخل في إطارها الأعمال الإرهابية التي تؤدي إلى توقف الجهاز عن العمل جزئيًا أو كليًا، وتخريب وسرقة قواعد البيانات.

طرق مواجهة تهديدات أمن المعلومات

- **تطبيق مبدأ أقل الامتياز (Principle of Least Privilege) :**

ويعني منح المستخدمين الحد الأدنى من الصلاحيات اللازمة لأداء مهامهم.

- **استخدام المصادقة متعددة العوامل "الثنائية" (Multi-Factor Authentication) :**

ويتطلب من المستخدمين تقديم أكثر من دليل واحد للتحقق من هويتهم.

- **تشفير البيانات (Data Encryption):**

ويحول البيانات إلى صيغة غير قابلة للقراءة إلا باستخدام مفتاح التشفير المناسب.

- **الجدران النارية (Firewalls):** وهي أنظمة تعمل كحاجز بين الشبكة الداخلية والشبكات الخارجية، وتقوم بفحص حركة المرور ومنع الوصول غير المصرح به.
- **أنظمة كشف ومنع الاختراق (Intrusion Detection and Prevention Systems):** وهي أنظمة تقوم بمراقبة الشبكة والأنظمة بحثًا عن أي نشاط مشبوه، وتقوم باتخاذ إجراءات لمنع وقوع الهجمات (IDS وIPS).
- **التوعية والتدريب:** تدريب الموظفين على أفضل ممارسات أمن المعلومات، مثل كيفية التعرف على رسائل التصيد الاحتيالي، وكيفية إنشاء كلمات مرور قوية.

- **اختيار موقع مناسب للأجهزة وتوفير مصدر احتياطي للطاقة الكهربائية:** لحماية الأجهزة من الكوارث.
- **نسخ احتياطي دوري للبيانات.**
- **تثبيت برامج مكافحة الفيروسات:** لحماية الأنظمة من البرمجيات الخبيثة.

لا توجد حماية تامة وكاملة، لكن هناك جتهزية دائمة

الأمن السيبراني

الأمن الحاسوبي أو الأمن السيبراني

أمن السايبر Cyber Security:

مجموعة من الممارسات والتقنيات المصممة لحماية **أنظمـــة المعلومـــات والشـــبكات والبيانـــات** مـن **الهجمـــات الإلكترونيـــة**، بهـدف ضـمان السـرية والنزاهة والتوفر للمعلومات الرقمية ووسائلها.

لكنه أيضًا...ثقافية ووعي وسلوك، لا مجرد برامج حماية.

أهم مرجعيات أمن المعلومات الوطنية والدولية

1- المرجع الوطني لأمن المعلومات (RNSI)

2- الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية (2025-2029)

3- الأيزو 27000 لأنظمة إدارة أمن المعلومات

1- المرجع الوطني لأمن المعلومات (RNSI)

وزارة البريد والمواصلات السلكية واللاسلكية

يكمن الهدف من وراء إعداد المرجع الوطني لأمن المعلومات RNSI في إقامة حوكمة ونهج موحّد لأمن المعلومات داخل الهيئات والمؤسسات. هذا المرجع يحدد الحد الأدنى من المتطلبات المتعلقة بالأمن، وذلك من أجل تسيير ومقاومة والتقليل من أثر التهديدات المتوقعة.

1- المرجع الوطني لأمن المعلومات (RNSI)

زيادة على ذلك، إن مرجع أمن المعلومات يقدم الضوابط الأمنية وأفضل الممارسات التي يجب أن تتبناها الهيئات العمومية، مع التركيز على تدريب وتوعية المستخدمين بالمخاطر التي تنطوي عليها، والتقييم الدوري للضوابط من أجل ضمان الاستجابة المستمرة للمتطلبات الأمنية والامتثال للالتزامات التنظيمية.

1- المرجع الوطني لأمن المعلومات (RNSI)

يجدر التذكير بأنه تم إطلاق النسخة الأولى من المرجع الوطني لأمن المعلومات عام 2016، والتي تضمنت سبعة (07) محاور:

الأمن المادي؛ مراقبة الدورية للأنظمة؛

إدارة المخاطر والقدرة على استعادة المعلومات بعد الحوادث.

إدارة الموجودات؛ أمن المستخدم النهائي؛

تأمين الشبكات؛ أمن الأنظمة؛

1- المرجع الوطني لأمن المعلومات (RNSI)

يتضمن المرجع الصادر في 2020 عشرين (20) مجالًا:

. إدارة الموجودات؛ . حماية البيانات ذات الطابع الشخصي؛

•إدارة ومراقبة النفاذ ؛ . أمن أجهزة المحمول؛

•أمن الشبكات؛ . أمن أنظمة المعلومات؛

•الأمن المتعلق بالتشغيل؛ .أمن أنظمة المعلومات بالغ الأهمية؛

•أمن الحوسبة السحابية؛ . التشفير؛

. الأمن المادي؛ . أنترنت الأشياء IoT؛

. المراقبة وتسجيل الوقائع؛ . إدارة الحوادث الأمنية؛

. تسيير استمرارية النشاطات؛ . الموارد البشرية؛

. الأمن المتعلق باستخدام مواقع التواصل الاجتماعي؛

. دمج الأمن خلال دورة حياة تطوير البرمجيات؛

. متطلبات الأمن لمشاريع تكنولوجيات الإعلام والاتصال؛

. العلاقة مع الأطراف الثالثة؛

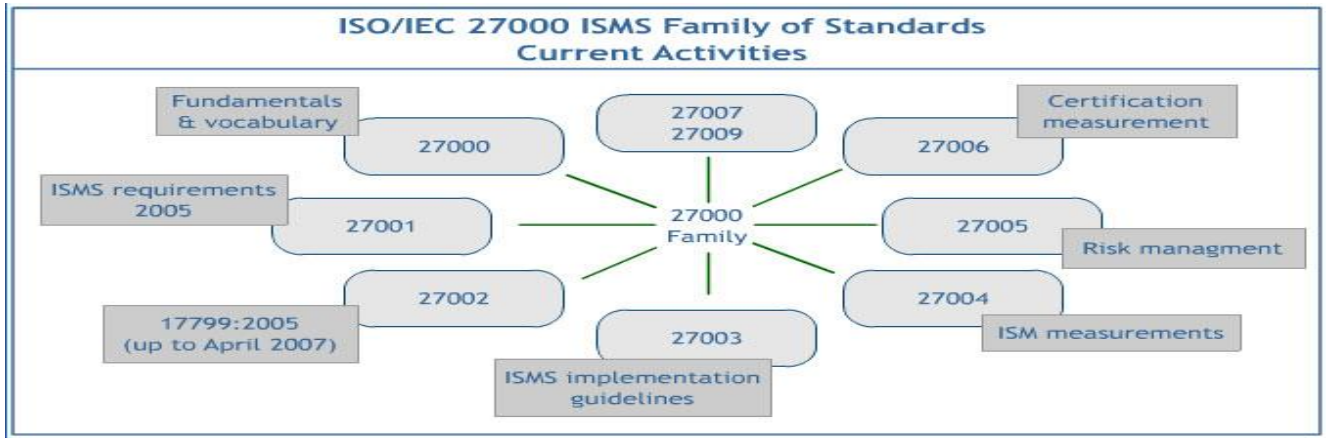
2- الأيزو 27000 لأنظمة إدارة أمن المعلومات

الايزو هو **الاسم المختصر لـ International Organization for Standardization** أي **"المنظمة الدولية لتوحيد المقاييس** منظمة التقييس الدولية، أو **ISO**، هي منظمة دولية مستقلة غير حكومية وغير ربحية، تعمل على تطوير ونشر معايير دولية موحدة تغطي مجموعة واسعة من الصناعات والقطاعات. يقع مقرها في جنيف، سويسرا، وتضم في عضويتها هيئات التقييس الوطنية من مختلف دول العالم.

المعهد الجزائري للتقييس: IANOR

2- الأيزو 27000 لأنظمة إدارة أمن المعلومات

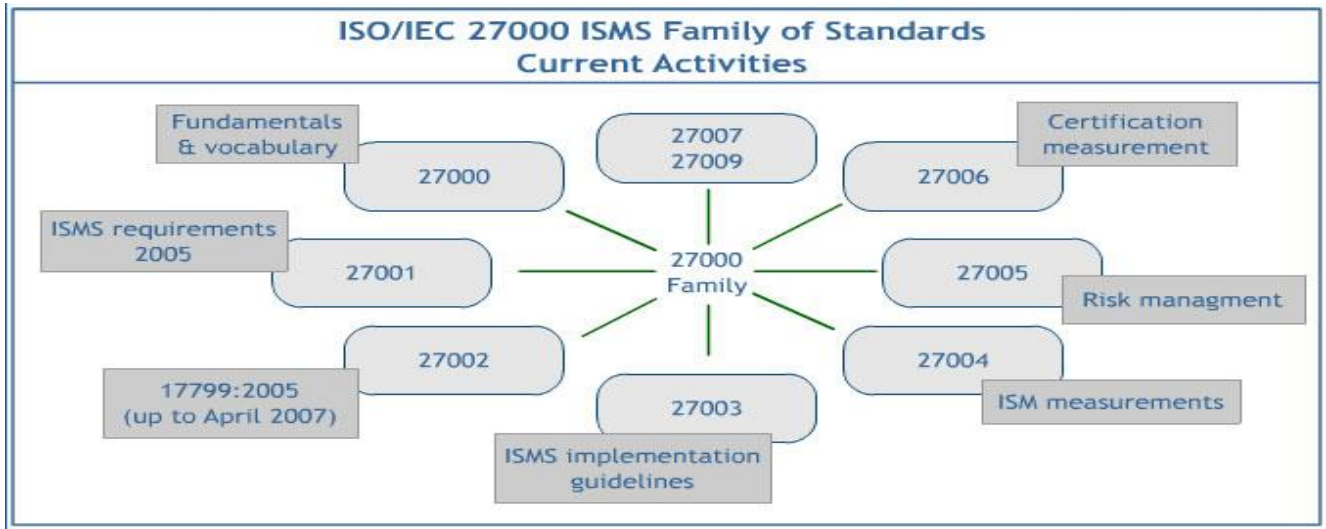
لقد ظهر تعبير نظم إدارة أمن المعلومات ISMS رسمياً كأحد معايير الجودة، وأحد مكونات النظم الإدارية مع ظهور معيار الأيزو ISO/IEC 17799 ويعرف أيضاً بالجزء الأول، ويحوي على 133 بنية معيارية مصنفة تحت أحد عشرة عنواناً رئيسياً، وبعد ذلك تتطور إلى المعيار ISO/IEC27002 ويعرف أيضاً بالجزء الثاني، وهو أحد أفراد عائلة نظم إدارة أمن المعلومات المعيارية ISO/IEC27000 الذي نشر لأول مرة عام 2000



ISO 27000

يُعتبر المعيار الأساسي الذي يحدد **المفاهيم والمصطلحات** المتعلقة بنظام إدارة أمن المعلومات.

يقدم نظرة شاملة عن أهداف ومعايير هذه العائلة.



2- الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27001

أهم معيار في العائلة، لأنه يحدد متطلبات إنشاء وتنفيذ وصيانة وتحسين نظام إدارة أمن المعلومات

هو المعيار الوحيد في العائلة الذي يمكن للمؤسسات أن تحصل على شهادة مطابقة له. يركز على:

- تقييم المخاطر الأمنية.
- وضع ضوابط لحماية البيانات.
- تحسين الإجراءات الأمنية باستمرار.

2- الأيزو 27000 لأنظمة إدارة أمن المعلومات

ISO 27002

يقدم **إرشادات عملية** حول كيفية تنفيذ ضوابط أمن المعلومات المحددة في المعيار ISO 27001. يحتوي على قائمة بأفضل الممارسات الأمنية مثل:

- التحكم في الوصول.
- إدارة الأصول.
- التشفير.

ISO 27003

يُركز على **إرشادات تطبيق ISO 27001.**

يساعد المؤسسات على فهم كيفية تصميم نظام إدارة أمن المعلومات

2- الأيزو 27000 لأنظمة إدارة أمن المعلومات

عائلة ISO 27000 ليست مجرد مجموعة من الوثائق، بل هي دليل شامل يساعد المؤسسات على تحقيق أعلى مستويات الأمان. إنها مرجع عالمي لكل من يسعى لفهم أو تطبيق نظام إدارة أمن المعلومات.

نهايـة العـرض

وشكـرًا لكـم