ثقافة أمن المعلومات

لغير العاملين في تقانة المعلومات

دائرة تكنولوجيا المعلومات
في
وزارة المالية

عناصر المحاضرة

- تعريف أمن المعلومات وأهميتها.
- مكونات وأركان النظام المعلوماتي.
- جرائم المعلوماتية وتصنيفها.
- المخترقون.
- وسائل الحماية.
- تعليمات استخدام واختيار كلمة المرور.
- القياس الحيوي.
- توصيات الملتقى الدولي الثالث لأمن المعلومات والاتصالات
- الخلاصة.

تعريف أمن المعلومات

يمكن تعريف أمن المعلومات من ثلاثة زوايا:

- **من الناحية الأكاديمية** : هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .
- **ومن الناحية التقنية**: هي الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .
- **من الناحية القانونية**: هي محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها ومكافحة أنشطة الاعتداء عليها أو استغلالها في ارتكاب جرائم معلوماتية.

تعريف أمن المعلومات

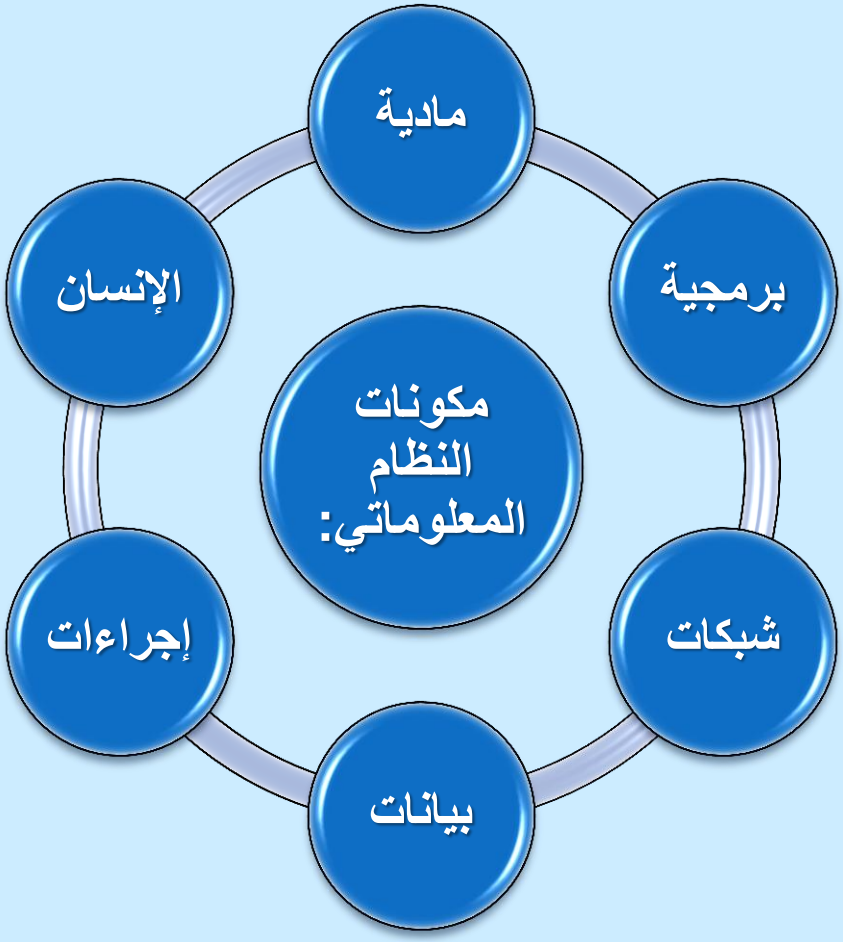
- وبشكل عام فإنه يقصد **بأمن المعلومات**:

" حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة)".

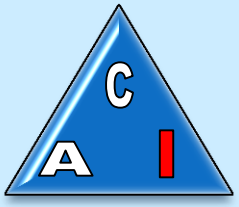
أهمية أمن المعلومات:

١. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.
٢. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر التي يمكن أن تظهر عند التعامل مع الأطراف الأخرى.
٣. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص والعام.
٤. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
٥. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
٦. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني.

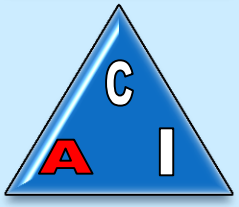
مكونات النظام المعلوماتي:



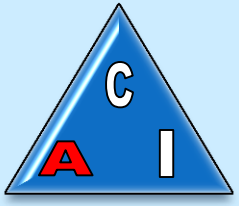
أركان أمن المعلومات :



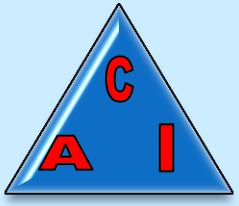
- أخطاء مدخلين



- حذف معلومات



- الحرمان من الخدمة



- الكراكر

جرائم المعلوماتية:

- هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.

- تُكبد جرائم المعلوماتية الحكومات والمنشآت خسائر تقدر بمليارات الدولارات سنوياً.

- في أحدى الدراسات التي أجريت على قطاع المصارف أن نسبة ٧٠% من هذه الجرائم تتم بتواطؤ المجرمين والمبرمجين وموظفي المصارف.

تصنيف جرائم المعلوماتية:

١. **جرائم هدفها نشر المعلومات:**

مثل الحصول على أرقام البطاقات الائتمانية، والحسابات المصرفية ومعلومات استخباراتيه.

٢. **جرائم هدفها نشر معلومات غير صحيحة:**

مثل نشر المعتقدات الخاطئة أو التشكيك في القرآن والسنة.

٣. **استخدام تقنية المعلومات كوسيلة لأداء الجريمة:**

مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.

٤. **جرائم لها علاقة بانتشار تقنية المعلومات:**

مثل قرصنة البرامج الأصلية والتي تكون أسعارها ٥٠٠٠$ لتباع بأقل من ١٠$

المخترقون:

- هم أشخاص يتمتعون بموهبة وقدرة عاليتين على كتابة وتصميم البرامج، وفهم عميق لكيفية عمل الحاسب الآلي مما يسهل عليهم اختراق أنظمتها وتغييرها.
- **هناك نوعين من المخترقين:**

الأول : الهاكر (White Hat).

هم في العادة أشخاص فائقو الذكاء يسيطرون بشكل كامل على الحاسب، ويجعلون البرامج تقوم بأشياء أبعد بكثير مما صممت له أصلا. لذلك نجد أن بعض الشركات العملاقة توظف أمثال هؤلاء الهاكر لتستفيد من مواهبهم سواء في الدعم الفني، أو حتى لإيجاد الثغرات الأمنية في أنظمة هذه الشركات.

الثاني: الكراكر(Black Hat).

هم من يسخرون ذكائهم بطريقة شريرة، وهم يهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة معلومات الآخرين الشخصية، ويغير أولئك المخربون، أحيانا، المعلومات المالية للشركات، أو يكسرون أنظمة الأمان، ويقومون بأعمال تخريبية أخرى.

المخترقون:

الفرق مابين الهاكر و الكراكر:

- **الكراكر:**

١. يمتلك القدرة على اختراق أنظمة التشغيل والبرامج الغير مجانية والتلاعب في برمجتها وإعطاؤها رقم خاص لكي تعمل.

٢. ويقوم بكسر الأنظمة الأمنية لأهداف تخريبية، فقد يكون هدفه سرقة معلوماتك أو في أسوأ الأحيان القضاء على النظام المعلوماتي الإلكتروني، بشكل كلي.

٣. كثير منهم يقوم بسرقة البرامج و توزيعها مجانا لهدف، فمنهم من يضع ملف الباتش بين ملفات هذا البرنامج.

٤. الكراكر دائما عمله تخريبي ولا ينفع سوى نفسه أو من يدفع له.

- **الهاكر:**

١. يحاول فقط أن يتعرف على كيفية عمل النظام والبرامج لكي يساعد في تطويرها وتحسينها.

٢. لديه القدرة الكاملة على اختراق أنظمة التشغيل عبر الانترنت.

٣. يقوم الهاكر بحل المشاكل و بناء الأشياء، و يؤمن بالعمل التطوعي.

٤. الهاكر دائما عمله بناء ومفيد و ينفع الآخرين.

أمثلة لمواقع مخترقة:وكالة الاستخبارات المركزية الأمريكية

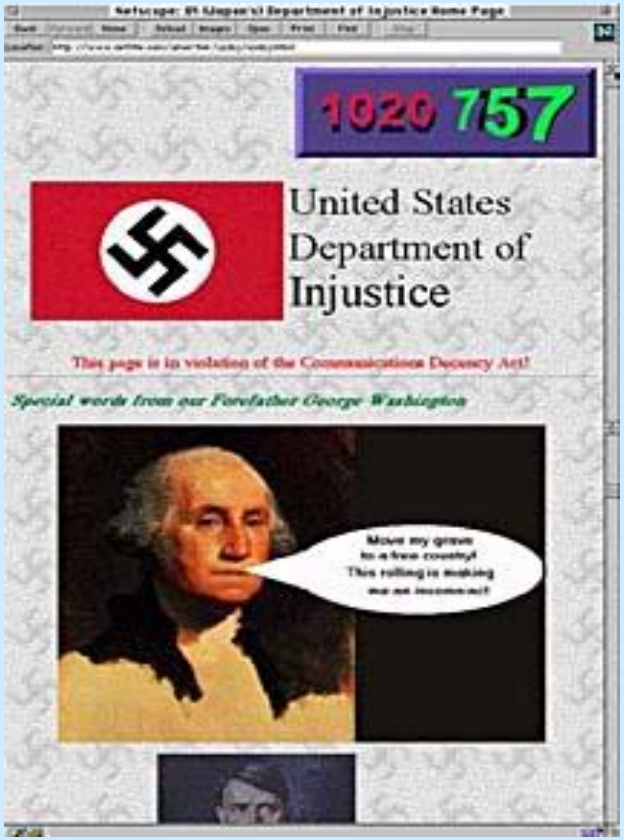
الموقع الأصلي

الموقع المخترق

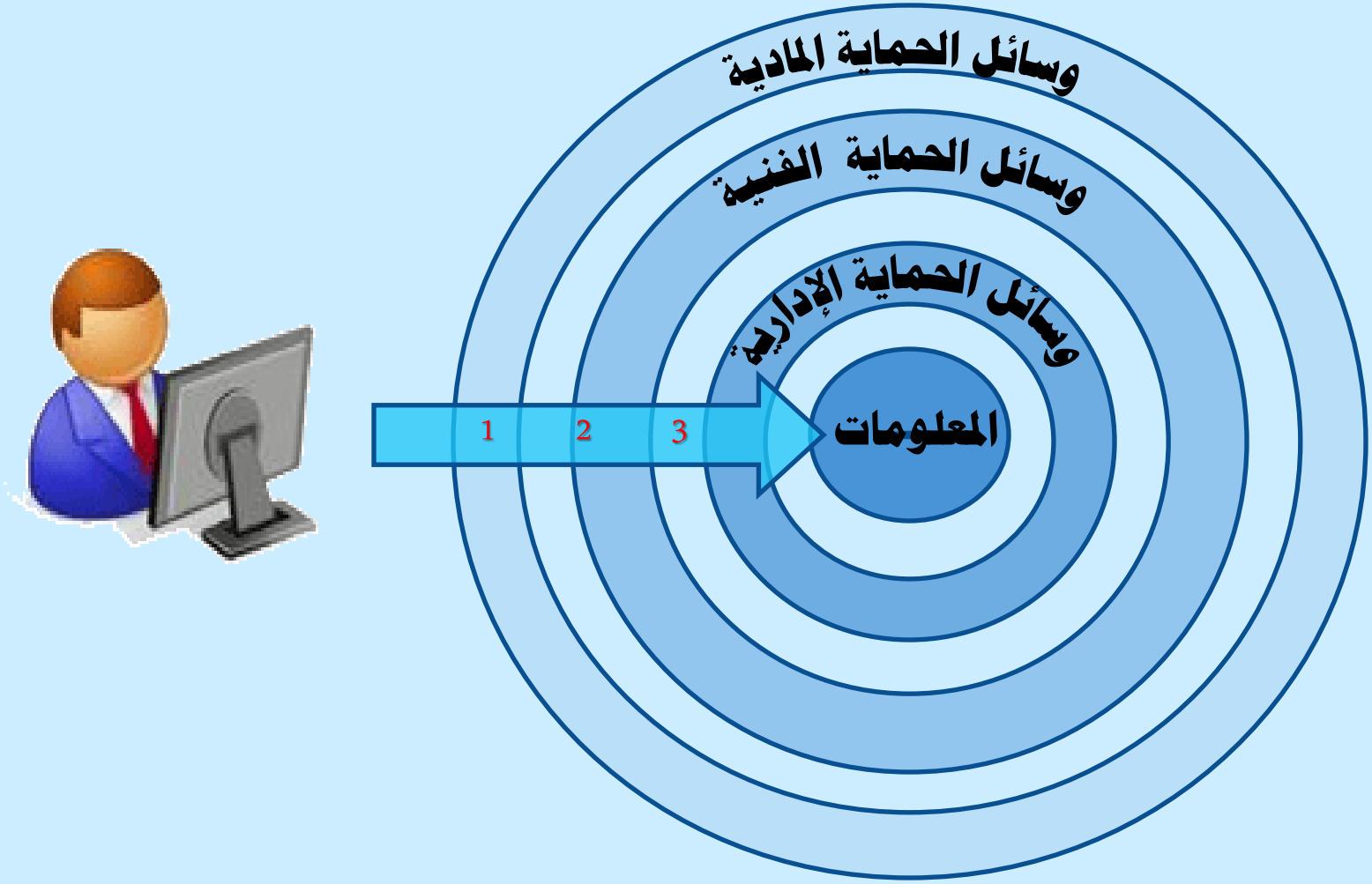
أمثلة لمواقع مخترقة:وزارة العدل الأمريكية.

الموقع الأصلي

الموقع المخترق



وسائل الحماية:



وسائل الحماية:

وسائل الحماية المادية:

وهي الأجزاء **المحسوسة** من وسائل الحماية.

من أمثلتها:

١. الكاميرات (الفيديو أو الفوتوغرافية)
٢. أجهزة الإنذار .
٣. الجدران والأسوار والمفاتيح.
٤. بطاقات دخول الموظفين.
٥. أجهزة اكتشاف الأصوات والحركة.

وسائل الحماية:

وسائل الحماية الفنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسئولياته.

من أمثلتها:

١. كلمة المرور.
٢. القياس الحيوي.
٣. التشفير.
٤. الجدران النارية.
٥. البرامج المضادة للفيروسات.
٦. التوقيع الالكتروني.

وسائل الحماية:

وسائل الحماية الإدارية:

وهي إعداد وصياغة سياسات أمن المعلومات وتتضمن:

- تشريعات داخل المنشأة لتنظيم أمن المعلومات وتحديد المسئوليات والأدوار.
- تحدد ما هو مسموح به وما هو غير مسموح به للتعامل مع المعلومات ومع نظم المعلومات.

من أمثلتها:

١. اتفاقية صلاحيات المستخدم وقبول استخدام النظام.
٢. الخصوصية.
٣. كلمات المرور.
٤. البريد الالكتروني.

وسائل الحماية:

- توعية الموظفين:

بما أن العنصر البشري يُعتبر من أهم مكونات النظام الأمني للمعلومات، فبالتالي يجب الحرص على تثقيفه وتوعيته عبر الطرق الآتية:

١. الاشتراك في مجموعات الاهتمام بأمن المعلومات.
٢. حضور عدد من المحاضرات القصيرة لمدة يوم أو نصف يوم في مجال أمن المعلومات ، ويكون حضورها إلزامي.
٣. تكريم الموظفين المثاليين بشكل شهري والذين طبقوا الأنظمة واللوائح.
٤. إقامة برامج تدريبية لكبار الموظفين وكذلك لمستخدمي الأجهزة و الإداريين.

تعليمات استخدام كلمة المرور:

- لاستخدام كلمة المرور:

١. أن تكون خاصة ولا يطلع عليها أحد مهما كان.
٢. عدم كتابتها أبدا سواء كان في الجوال أو على ورق الملاحظات.
٣. يجب تغييرها كل شهرين كحد أقصى.
٤. لا تستخدم نفس كلمة المرور في حسابات وأماكن أخرى.
٥. لا تقبل أن يضع لك شخص أخر كلمة المرور.
٦. عندما تشعر بأن أحد اكتشف كلمة المرور، قم بتغيرها فوراً.
٧. عند إدخالك لكلمة المرور تأكد بأنه لا يوجد أحد يراقبك.
٨. تجنب استخدام الحواسيب المشتركة مع الآخرين.

تعليمات اختيار كلمة المرور:

- لاختيار كلمة المرور:

١. يُفضل أن تحتوي على أحرف وأرقام.
٢. يُفضل أن لا تقل عن ٨ خانات للمستخدم الغير تقني.
٣. يُفضل أن لا تكون مشهور ومتداولة.
٤. يمكن استخدام معادلة بسيطة لإنشاء كلمة المرور، مثلاً

نضع حرف ، ثم الرقم الأول، ثم الرقم التالي يكون ثلاثة أضعاف الرقم السابق وهكذا.

1*3=3 **9*3=27**

A	1	#	3	W	9	$	7

3*3=9

القياس الحيوي Biometrics:

- **BioMetrics**هي كلمة إغريقية مكونة من جزئين "BIO" ومعناها الحياة و "METRICS" ومعناها قياس.

- والتعريف الدقيق **للقياس الحيوي** : هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة.

القياس الحيوي:

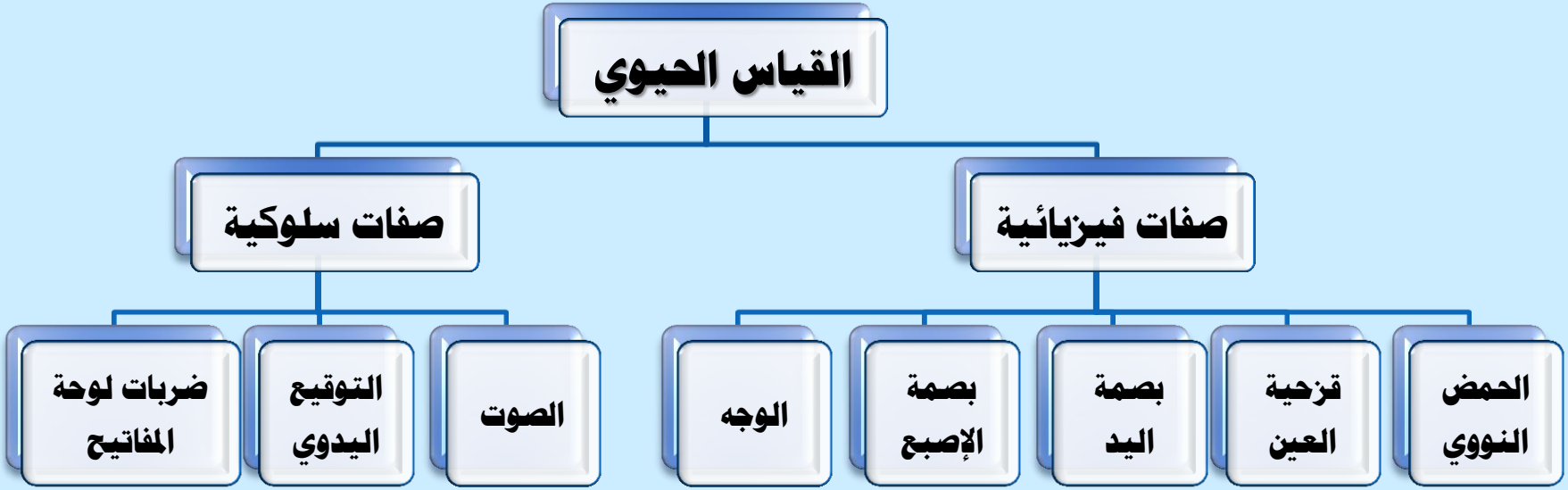
أقسام القياس الحيوي:.

١.الصفات الفيزيائية:

وهي الصفات التي تتعلق بجزء من جسم الإنسان.

٢.الصفات السلوكية:

وهي الصفات التي تتعلق بسلوك الإنسان.



القياس الحيوي:

* يوفر لنا القياس الحيوي عدد من المزايا منها:

١. **الأمن والخصوصية:**

- يمنع الأشخاص الآخرين من الدخول الغير مصرح على البيانات الشخصية.
- إيقاف سرقة الهوية،مثل استخدام البطاقات الائتمانية أو الشكيات المسروقة.

٢. **البديل لحمل الوثائق الثبوتية مثل:**

- بطاقة الهوية الوطنية. - رخصة القيادة. - بطاقة الائتمان أن وجدت.

٣. **البديل لحفظ وتذكر الأرقام السرية.**

٤. **البديل لحمل المفاتيح للدخول إلى:**

- السيارات. - المنازل. -المكاتب.

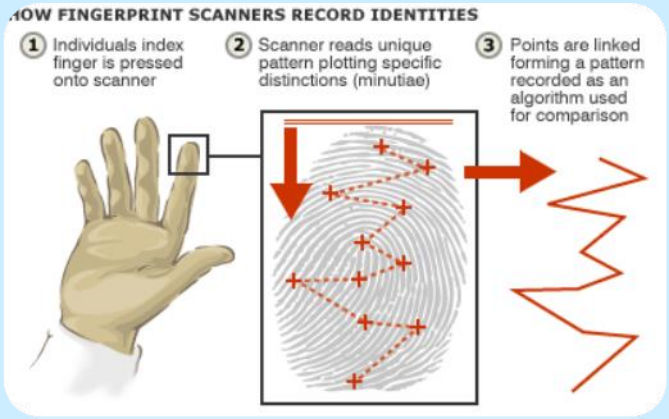
٥. **تأمين سرية العمليات المالية مثل:**

-مكائن الصراف الآلي ATM - التجارة الإلكترونية.

القياس الحيوي:

- **بصمة الإصبع Fingerprint Scanning:**

أكثر الأنظمة شيوعًا في الاستخدام وخاصة بين المستخدمين لأجهزة تقنية المعلومات .بصمة الإصبع تمسح ضوئيًا باستخدام قارئات خاصة، ومن الأمثلة على هذه القارئات :أجهزة تربط بالكمبيوتر ، أو تأتي مدمجة مع الفأرة.



القياس الحيوي:

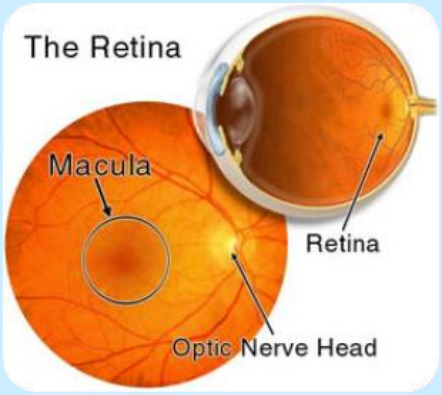
- **بصمة اليد Hand Geometry:**
- يُستخدم هذا النظام منذ سنوات عديدة وبشكل خاص في أنظمة متابعة الحضور والانصراف وتسجيل الوقت .يعطي هذا النظام توازنًا جيدًا بين الأداء والدقة وسهولة الاستخدام .ومن السهولة دمجه في أنظمة أخرى .توضع اليد على الجهاز الماسح في المكان المخصص لها، ويقوم النظام بفحص تسعين صفة من بينها شكل اليد ثلاثي الأبعاد 3D، طول وعرض الأصابع، وكذلك شكل مفاصل الأصابع.

القياس الحيوي:

- **قزحية العين Iris Scanning:**
- يعتمد النظام المستخدم لقزحية العين على ثباتها حيث أنها الجزء الذي لا يتغير من الجسد .ولها ميزة أيضًا أنها مرئية عن بعد، ليست كصفة الشبكية .أيضًا قزحية العين اليسرى تختلف عن العين اليمنى لنفس الشخص.، ولا يحتاج المستخدم أن يقرب هذه العدسات من عينه، وهي بالتالي تعطي دقة عالية مع سهولة الاستخدام.

القياس الحيوي:

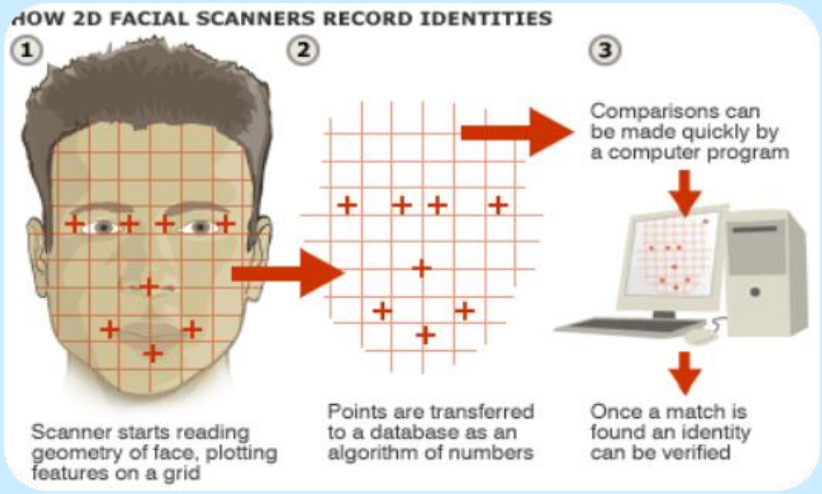
- **شبكية العين Retina Scanning:**
- هذه الطريقة تستخدم مصدر ضوء منخفض لعمل مسح للشعيرات الدموية خلف العين. عيب هذه الطريقة أن المستخدم يجب أن ينظر ويركز على الماسحة وهذا يسبب للمستخدم عدم الرغبة للتعامل مع النظام.



القياس الحيوي:

- **الوجه Facial Scanning:**

هذا النظام يعتمد على أخذ صورة كاملة للوجه من آلة تصوير، وقيام النظام بمقارنتها مع ما خزن فيه مسبقًا .مازالت هذه التقنية في أوج التطوير، وما هو موجود حالياً من الأنظمة المعتمدة على صورة الوجه لا تعطي دقة عالية.



القياس الحيوي:

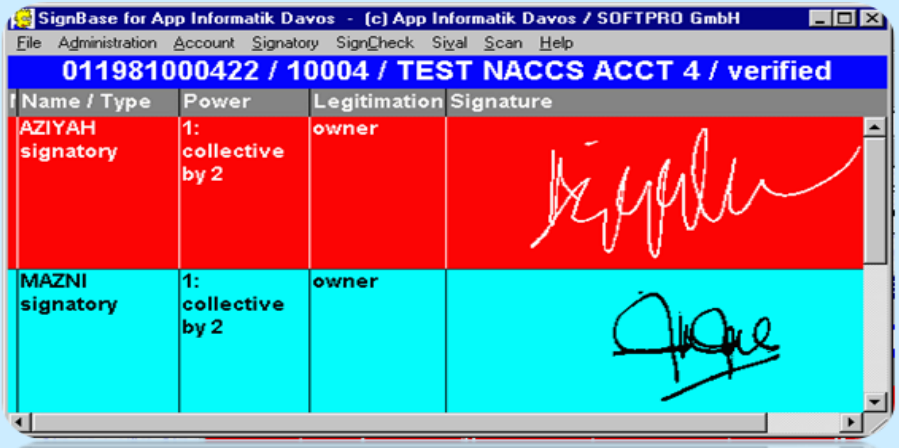
- **الصوت Voice Verification:**

في هذه الأيام، برامج تدقيق الصوت تعد من الإضافات الشائعة لأجهزة الكمبيوترات الخاصة لدى معظم الشركات والبنوك .لكن أنظمة القياس الحيوي المعتمدة على الصوت، فإنها تحلل ترددات الصوت بشكل أكثر دقة لكي تعطي نتائج صحيحة يُعتمد عليها .ولذلك يجب أن تكون بيئة هذا النظام هادئة، حيث أن أي ضجة تؤثر على النتيجة و أجهزة هذا النظام قد تكون مستقلة بحد ذاتها أو مدمجة مع أنظمة الهاتف التي قد تساعد في مجالات عديدة منها الأنظمة المصرفية.

القياس الحيوي:

- **التوقيع اليدوي Signature Verification:**

هذا النظام يعتمد على الطريقة التقليدية لتوقيع الشخص، ولكنها تتم من خلال توقيع الشخص على شاشة حساسة للمس باستخدام قلم ضوئي. ويتم من خلالها تحويل توقيعه إلى شكل رقمي ومن ثم مقارنته مع ما خزن مسبقًا في النظام.



القياس الحيوي:

- **الحمض النووي DNA Scanning:**

هذا النظام يعتمد على الشريط الوراثي للشخص DNA. وهو نظام معقد جدًا ويستحيل تغييره بين الأشخاص، وهذا النظام مكلف جدًا لذلك قليلاً ما يُستخدم.

القياس الحيوي:

- **ضربات لوحة المفاتيح keystroke Dynamics:**

هذا النظام يقوم تسجيل ضربات الشخص على لوحة المفاتيح .ومن خلال هذه العملية يقوم بمراقبة الوقت بين ضرب مفتاح والانتقال الأصابع لضرب مفتاح آخر. وكذلك يراقب الوقت الذي يأخذه المستخدم وهو ضاغط على المفتاح .وحيث أنه يجب على المستخدم أن يتذكر أسم المستخدم والرقم السري.

توصيات الملتقى الدولي الثالث لأمن المعلومات والاتصالات

١. وضع سياسة واضحة لأمن المعلومات على مستوى الدولة، وعلى مستوى المؤسسات.
٢. تحديد الاحتياجات الفعلية للمجتمع في مجال أمن المعلومات، والعمل على رفع الكفاءة لدى الكوادر المعلوماتية في هذا المجال.
٣. تشجيع البحوث في مجال التعمية والتشفير وغيرها من مجالات أمن المعلومات في الجامعات ومراكز البحوث المحلية .
٤. وضع إطار عام على مستوى الدولة لتمويل متطلّبات أمن المعلومات.
٥. مساعدة القطاع الخاص على توفير خدمات أمنية للشركات والمؤسسات، وتقديمها على مستوى عالٍ، بطريقة تناسب الاحتياجات والتوقعات.

الخلاصة:

- أهمية التوعية ونشر ثقافة أمن المعلومات بين جميع شرائح المجتمع.
- لا يوجد أمن كامل في أي نظام.
- الأمن يتناسب عكسيا مع سهولة استخدام النظام.
- الأمن كالسلسلة، تقاس قوتها بقوة أضعف حلقة فيها.
- العنصر البشري من أهم العناصر الأمنية لان اختراق البشر أسهل من اختراق الأجهزة.
- الهاكر يُفيدون النظام الأمني بعكس الكراكر يهدمون النظام الأمني.
- يجب الاهتمام بتوفر المعلومات كجزء من الأمن.
- أهمية معرفة كيفية اختيار واستخدام كلمات المرور.
- ايجاد أنظمة رادعة لكل من يحاول العبث بأمن الدولة وأمن المستخدمين.
- وجود تشريعات خاصة بتقانة المعلومات ومكافحة الجرائم الألكترونية.