دورة تدريبية في :

أمن تكنولوجيا المعلومات

It security

المدرب:

برهان جنبلاط

- إجازة في الرياضيات التطبيقية – شعبة انفورماتيك

- رئيس دائرة الصيانة في قسم المعلوماتية .
- مدرب على مواضيع الرخصة الدولية لقيادة الكمبيوتر ICDL منذ العام ٢٠٠٣

الأمن المعلوماتي (المفاهيم والمصطلحات)

- المعلومات نوعان :
  - معلومات إلكترونية (Electronic Form Information)
  - تحفظ باستخدام التكنولوجيا الإلكترونية (مثل الحاسب الآلي).
  - معلومات تقليدية (Traditional Form Information)
  - تحفظ باستخدام الوسائل التقليدية(مثل الورق).

الأمن المعلوماتي (المفاهيم والمصطلحات)

- المعلومات الإلكترونية معرضة للعطب والهجوم أكثر من المعلومات التقليدية للأسباب التالية:
  - إمكانية تسرب المعلومات الإلكترونية.
  - المعلومات الإلكترونية غير ظاهرة للعين.
  - المعلومات قد تحفظ باستخدام وسائل صغيرة الحجم.
  - صعوبة التخلص من المعلومات.
  - صعوبة التعامل مع الحاسب الآلي.
  - تزايد الاتصالات والشبكات.

الأمن المعلوماتي (المفاهيم والمصطلحات)

- الصور التي تتنقل فيها المعلومات:
  - عبر وسائط التخزين (القرص الصلب ، القرص المرن ،القرص المضغوط ...)
  - عبر الأسلاك (الشبكات ، الهاتف ...)
  - لاسلكي(الأمواج الكهرومغناطيسية ، الأشعة تحت الحمراء...)

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**:

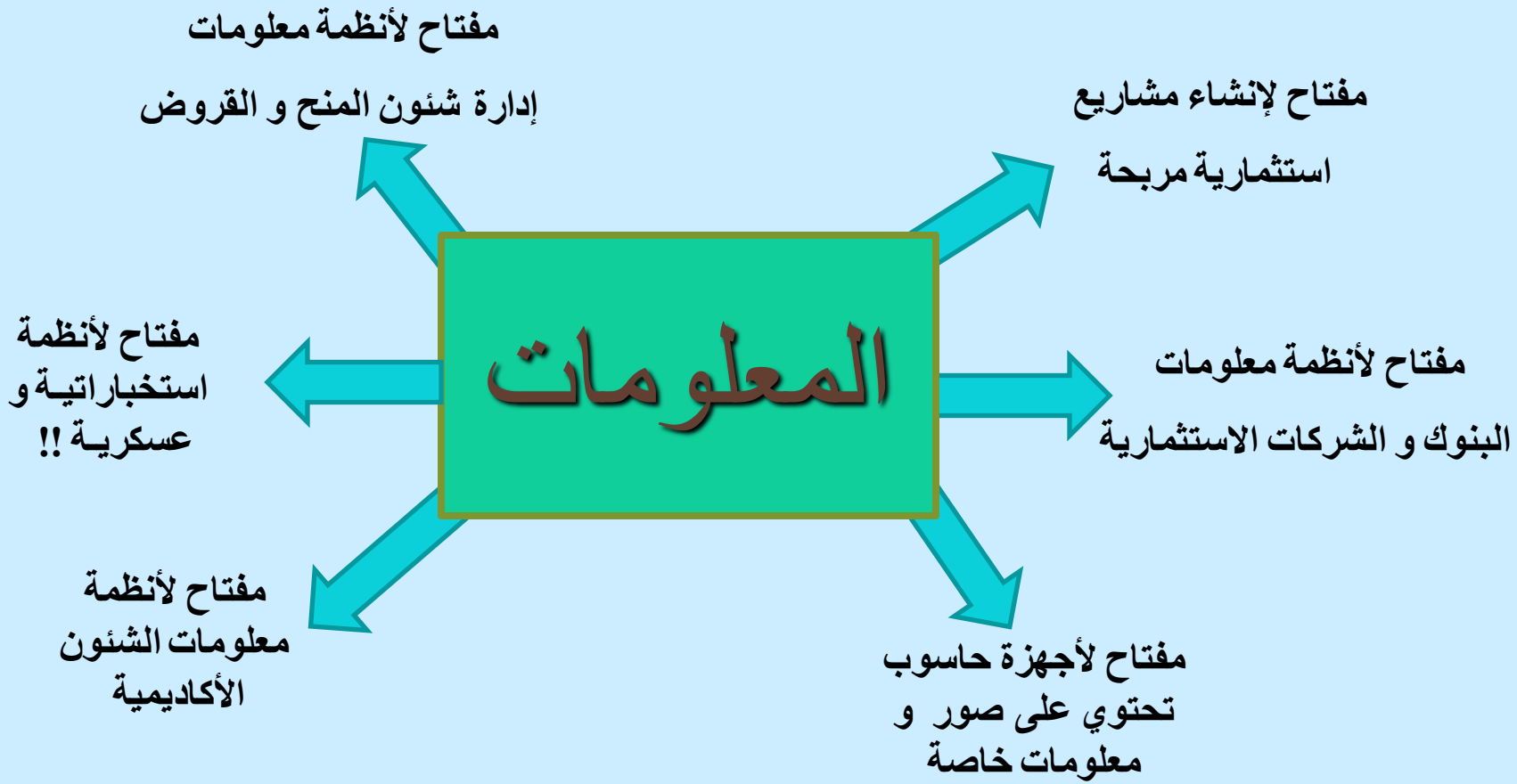
" حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة)".

تعريف أمن المعلومات

إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، و عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة على السماح لشخص ما بالوصول إلى معلوماتك الخاصة.

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

أهمية أمن المعلومات



أهمية أمن المعلومات

- الحاجة المتزايدة لإنشاء **بيئة إلكترونية آمنة** تخدم القطاعين الخاص والعام.
- النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
- الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
- مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً **للإجرام الإلكتروني**.

أهم اهداف أمن المعلومات

- معالجة الأخطاء المتعمدة وغير المتعمدة أثناء تصميم وبناء و تشغيل الأنظمة.
- منع سرقة أو اكتشاف المعلومات لغرض تغييرها بشكل غير قانوني.
- الحفاظ على المعلومات المتواجدة في اي نظام من الضياع أو التلف و من أخطاء الاستخدام المتعمد أو العفوي والكوارث الطبيعية و أخطاء الأجهزة و أخطاء البرمجيات.

بناء نظام أمن المعلومات

- مؤشرات مهمة يجب اخذها بعين الاعتبارعند بناء نظام أمني للمعلومات :

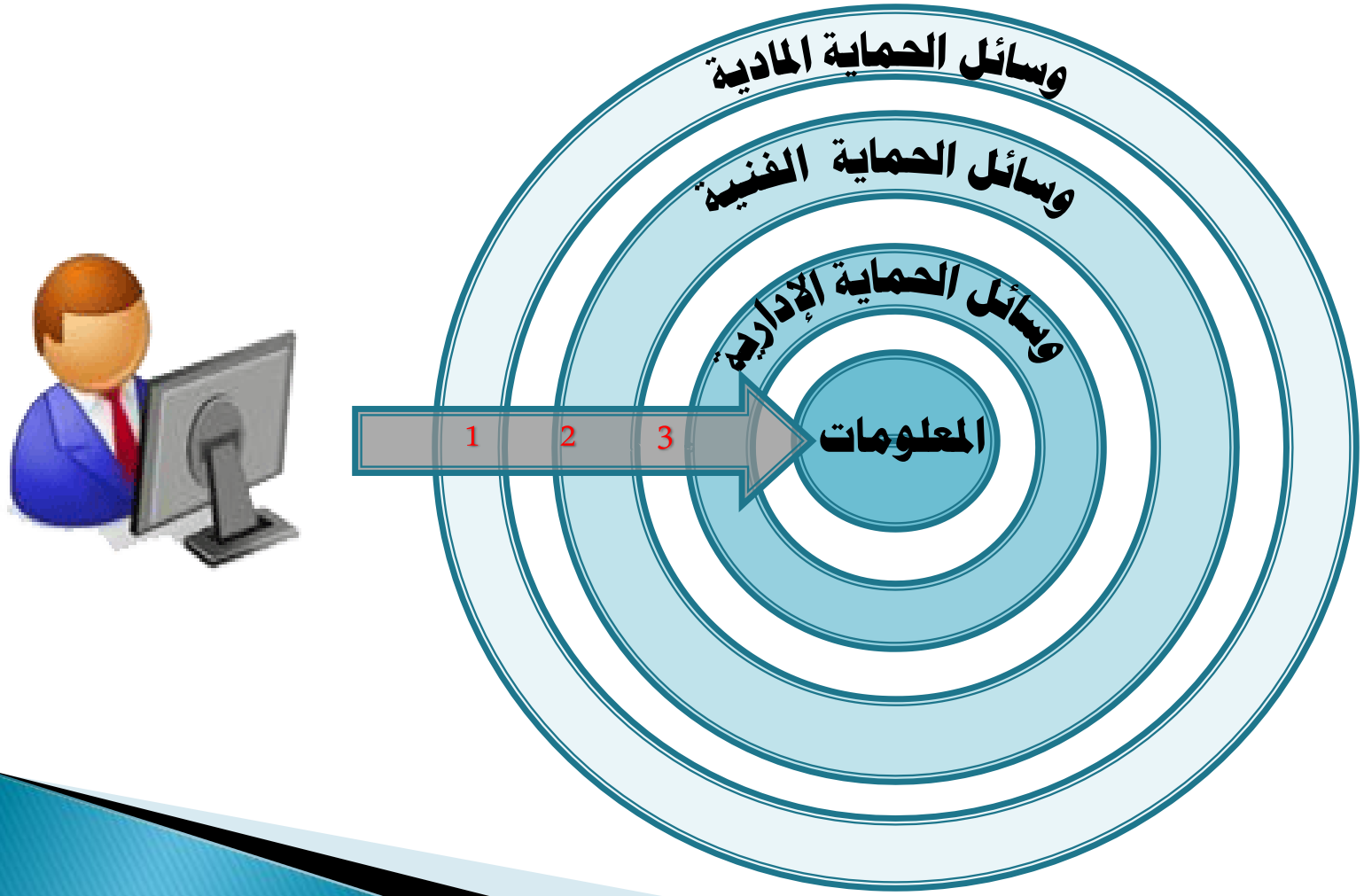
- ✓ يجب تحديد درجة الأمن المطلوبة للمعلومات التي سيتعامل معها النظام .
- ✓ كما يجب تحديد انواع المعلومات المتواجدة و تصنيفها حسب اهميتها.
- ✓ يجب تقدير كفاءة الأشخاص أو الجهات المحتمل محاولتها انتهاك الاجراءات الأمنية للنظام بطرق واساليب مختلفة غير مشروعة.

بناء نظام أمن المعلومات

- ✓ وضع ميزانية تأخذ بالأعتبار كافة التكاليف التي تؤدي الى وضع النظام الأمني.
- ✓ يجب تحديد و تقدير الأضرار التي من الممكن ان تصيب تلك المؤسسة في حالة فقدان او كشف او تلف لمحتويات النظام.

أركان التعامل مع المعلومات

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.

كلمة المرور Password

هي مجموعة من الرموز التي تسمح للدخول إلى الحاسوب، أو الموارد على شبكة الاتصال أو المعلومات.

فوائد كلمة المرور:

- تسمح للمستخدمين المصرح لهم فقط لدخول النظام
- إدارة و تحديد هوية الأشخاص بفاعلية و التدقيق في عملية الوصول.
- حفظ و حماية المعلومات
- حماية المعلومات الشخصية الخاصة بك.

نصائح لإنشاء كلمات المرور

كلمة المرور مسؤولية مالكها، لذا يجب عليه أن يتبع النقاط التالية عند إنشاء كلمة مرور:

١. يجب أن يكون تخمينها صعب
٢. يجب ألا يكون طولها اقل من (٨) أحرف
٣. يجب أن تتسم بميزة التعقيد، و التي ينبغي أن تحتوي على خليط من الأرقام و الأحرف و الرموز الخاصة مثل (*/-@+$)
٤. يجب أن لا تحتوي على اسم المستخدم
٥. يجب أن لا تحتوي كلمة المرور على معلومات شخصية مثل رقم الهاتف، أو اسم أحد الأقارب، أو تاريخ الميلاد

تعليمات اختيار كلمة المرور:

- لاختيار كلمة المرور:

١. يُفضل أن تحتوي على أحرف وأرقام.
٢. يُفضل أن لا تكون مشهور ومتداولة.
٣. 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				

نصائح للاستخدام كلمات المرور

١. لا تفصح عن كلمات المرور لأي شخص
٢. لا تستخدم نفس كلمة المرور للعمل في مواقع متعددة مثل البريد الإلكتروني أو الحاسب المصرفي
٣. لا تكتب أو تحفظ كلمة المرور على ورقة أو في رسالة بريد الالكتروني
٤. لا تستخدم خاصية تذكر كلمة المرور المتوفرة في بعض أنظمة التشغيل
٥. قم بتغير كلمة المرور بشكل دوري

البرامج الخبيثة The Malicious Software

هي أحد تهديدات الحاسوب في هذا العصر. ونقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض. و الأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.و يمكن يتصنيف أنواع البرمجيات الخبيثة على النحو التالي:

١. الفيروسات (Viruses)
٢. الديدان (Worms)
٣. برامج التجسس (Spywares)
٤. الخداع (Hoax)
٥. عمليات الاحتيال واصطياد الضحايا The Phishing Scam
٦. أحصنة طروادة Trojan Horses

الفيروسات Viruses

- فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة ، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة ، كما تقوم بالتلاعب بمعلومات الكمبيوتر المخزنة
- ينتقل الفيروس إلى جهازك عندما تقوم بنقل ملف ملوث بالفيروس إلى جهازك أو عند زيارة احد المواقع المشبوهة او اثناء تبادل السي ديات أو الفلاشات مع الأصدقاء و ينشط الفيروس عند محاولة فتحه ويمكن ان يصلك ايضا عن طريق البريد الألكتروني على هيئة مرفقات

الديدان Worms

- ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها
- يمكن أن تسبب الضرر بشكل واسع.
- على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة.

الديدان تعتبر برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

برامج التجسس Spywares

- هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة. في حالة التجسس، المستخدم يجهل هذا الغزو.
- يمكن لبرامج التجسس جمع ونقل المعلومات الشخصية.
- المعلنين وغيرهم يرغبون في معرفة ماهي المواقع الإلكترونية التي يقوم المستخدمون بزيارتها وما هي عادات وأساليب تصفح الإنترنت لديهم.
- في بعض الأحيان تقوم برامج التجسس بإعادة توجيه مدخلات المتصفح لتوجه المستخدم إلى موقع آخر غير المقصود.
- بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية

أحصنة طروادة The Trojan Horses

- وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة. تقوم بخداع المستخدمين من أجل تحميلها وتطبيقها على أنظمتهم.
- فيتم بذلك تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار

أضرار الإصابة بالفيروسات و البرامج الخبيثة

١. تعطيل الحاسوب
٢. ظهور شاشة الموت الزرقاء
٣. سرقة النقود إلكترونيا
٤. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات
٥. تسرق البيانات
٦. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات
٧. تبطئ الحاسب
٨. تبطئ الاتصال بالانترنت

أعراض الإصابة بالفيروسات و البرامج الخبيثة

- تباطؤ أداء الحاسوب.
- زيادة حجم الملفات، أو زيادة زمن تحميلها للذاكرة .
- ظهور رسائل تخريبية على الشاشة، أو الرسوم أو صدور بعض الأصوات الموسيقية.
- حدوث خلل في لوحة المفاتيح كأن تظهر على الشاشة أحرف ورموز غير التي تم ضغطها أو حدوث قفل للوحة المفاتيح .
- ظهور رسالة ذاكرة غير كافية لتحميل برنامج كان يعمل سابقاً بشكل عادي.
- سعة الأقراص أقل من سعتها الحقيقية.

الفيروسات

- **بعض طرق الحماية:**
  - برامج مكافحة الفيروسات مثل:

(Macafee , Kaspersky, Norton, Avira, AVG, NOD32)

  - توفير نسخ احتياطية (backup) .
  - جدار الحماية.
  - كلمة المرور(Password).

نصائح عند فتح ملحقات البريد الإلكتروني

- لا تفتح أية ملفات ملحقة ببريد إلكتروني من مصدر غير موثوق.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني ما لم تعرف محتواها.
- لا تفتح أية ملفات ملحقة ببريد إلكتروني إذا كان حقل الموضوع مشكوكاً فيها وغير متوقع.
- احذف سلسلة رسائل البريد الغير هامة وتجنب الرد عليها.
- لا تقم بتحميل أية ملفات من الغرباء.
- توخي الحذر عند تحميل الملفات من الانترنت، تحقق من شرعية المصدر وحسن سمعته.

الهدف من إعداد البرامج الخبيثة

- تختلف دوافع إعداد الفيروسات فمنها الدوافع الحسنة ومنها الدوافع المادية ومنها الدوافع الانتقامية ، فبعض الناس يقوم بإعداد الفيروسات للتسلية أو ولإظهار القدرة على البرمجة ولكن هناك من يعدها لهدف مادي وذلك لضمان تردد المستخدم لمحلات الكمبيوتر للصيانة او التخلص من هذا الفيروس او السطو على حسابات البنوك او المعومات العامة للشركات والمؤسسات الكبرى ، ومهما كان هدف اعداد الفيروس لابد من الوقاية منه لأنه يسبب الكثير من المشاكل والخسائر لمستخدمي الكمبيوتر .

القياس الحيوي Biometrics:

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

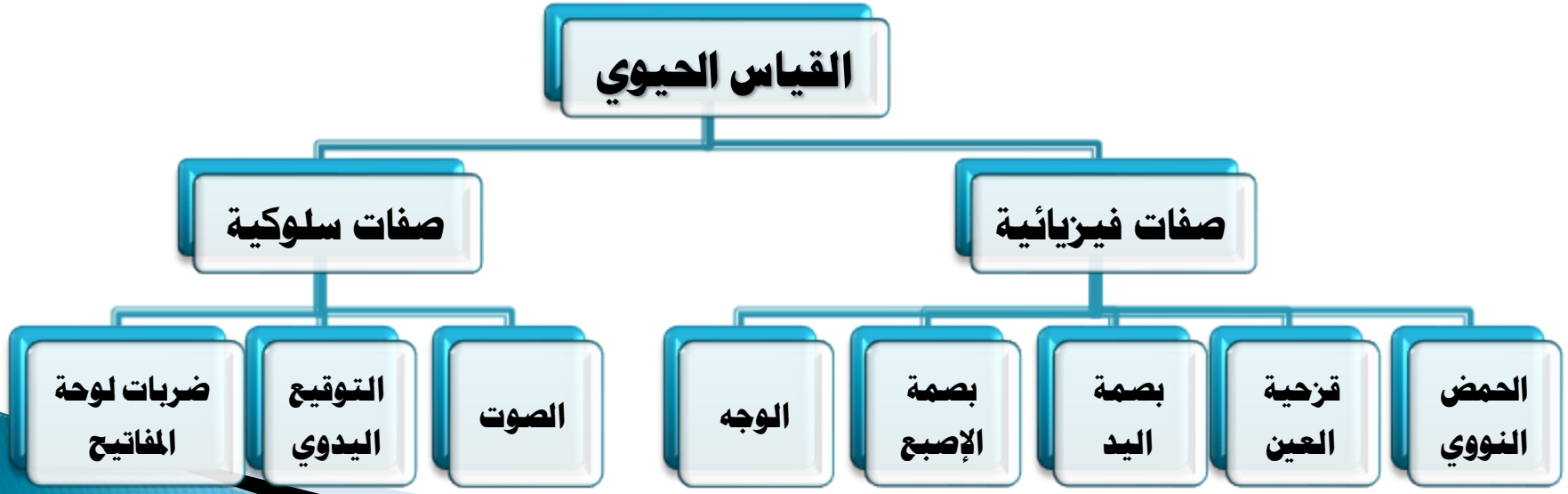
- والتعريف الدقيق **للقياس الحيوي** : هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة.

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.

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

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

- السيارات. - المنازل. -المكاتب.

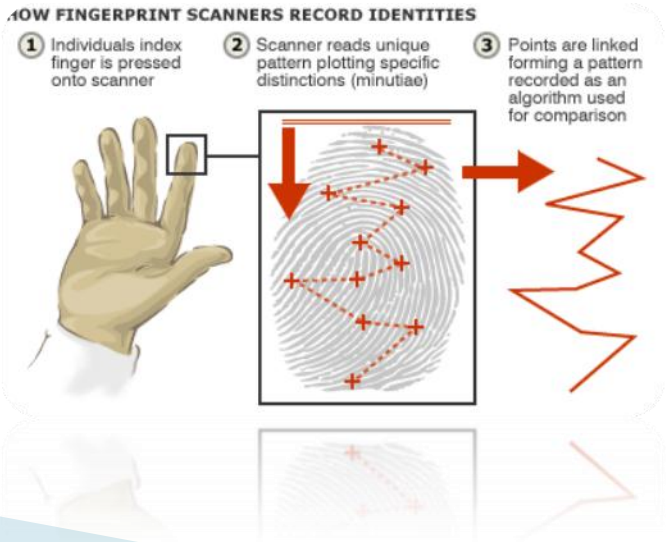
٥. **تأمين سرية العمليات المالية مثل:**

-مكائن الصراف الآلي ATM - التجارة الإلكترونية.

القياس الحيوي:

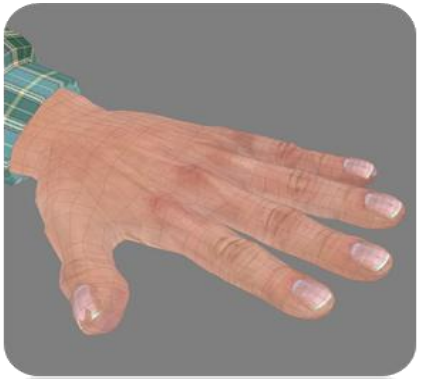
- **بصمة الإصبع Fingerprint Scanning:**

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.

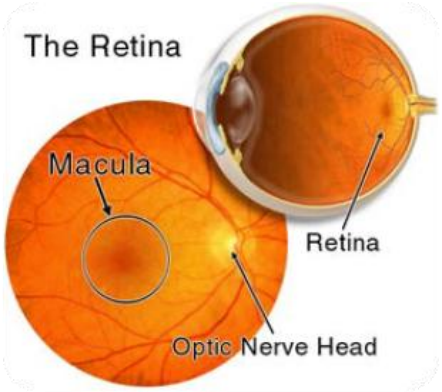


القياس الحيوي:

- **<u>قزحية العين Iris Scanning:</u>**
- 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:

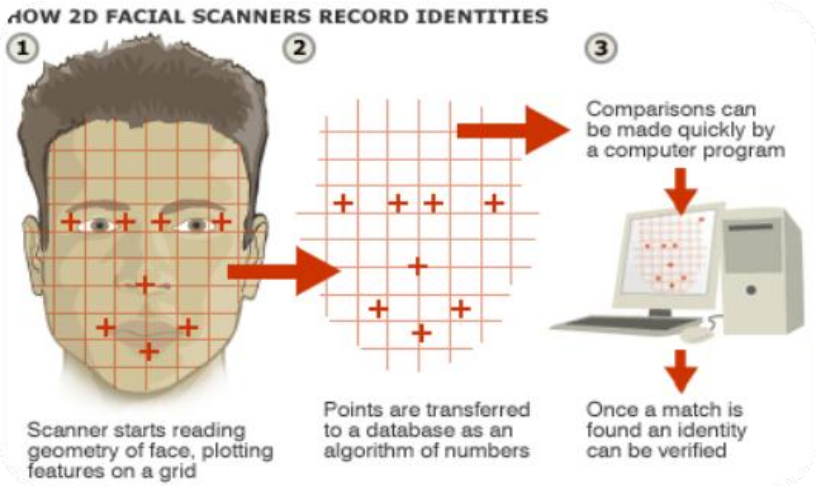
- **شبكية العين Retina Scanning:**
- هذه الطريقة تستخدم مصدر ضوء منخفض لعمل مسح للشعيرات الدموية خلف العين. عيب هذه الطريقة أن المستخدم يجب أن ينظر ويركز على الماسحة وهذا يسبب للمستخدم عدم الرغبة للتعامل مع النظام.

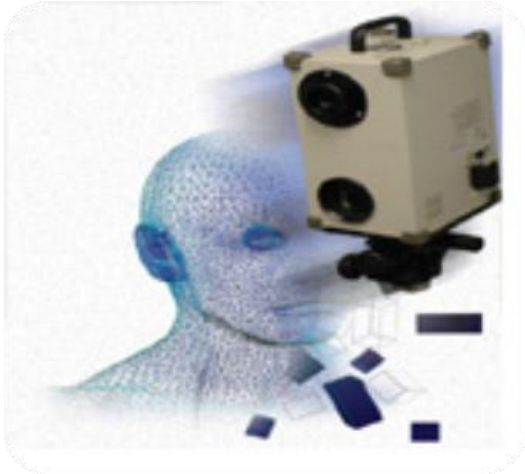


القياس الحيوي:

- **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.

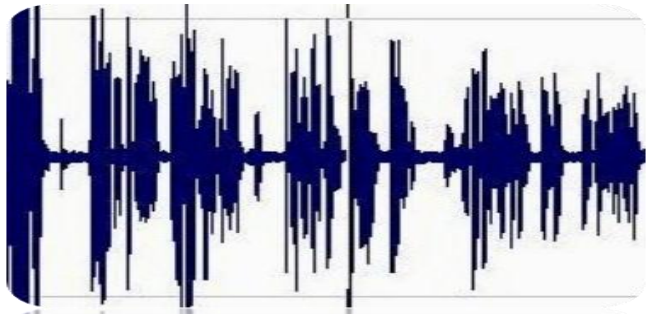




القياس الحيوي:

- **الصوت Voice Verification:**

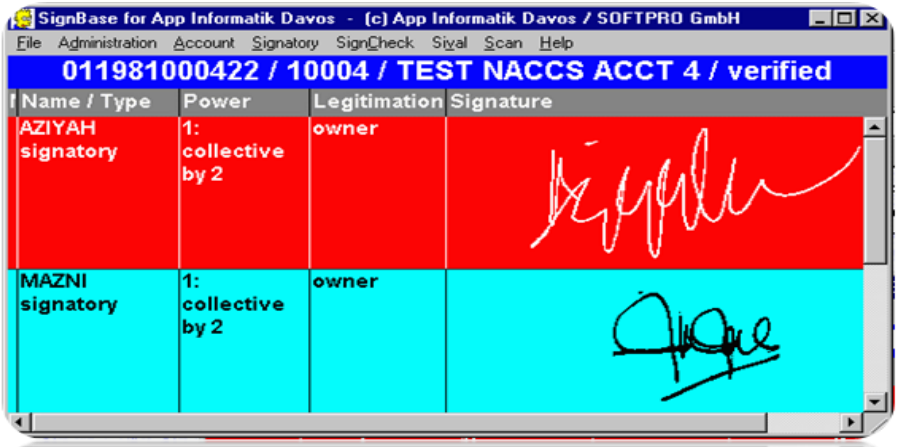
في هذه الأيام، برامج تدقيق الصوت تعد من الإضافات الشائعة لأجهزة الكمبيوترات الخاصة لدى معظم الشركات والبنوك .لكن أنظمة القياس الحيوي المعتمدة على الصوت، فإنها تحلل ترددات الصوت بشكل أكثر دقة لكي تعطي نتائج صحيحة يُعتمد عليها .ولذلك يجب أن تكون بيئة هذا النظام هادئة، حيث أن أي ضجة تؤثر على النتيجة و أجهزة 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.