معرفة سُبل حماية خصوصية معلوماتك وأجهزتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع، والذي يلحق الضرر بك ماديا أو معنويا

التعرف على مفهوم الامن الرقمي

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.

بعض العلامات التي تدل على اختراق الجهاز، ومنها

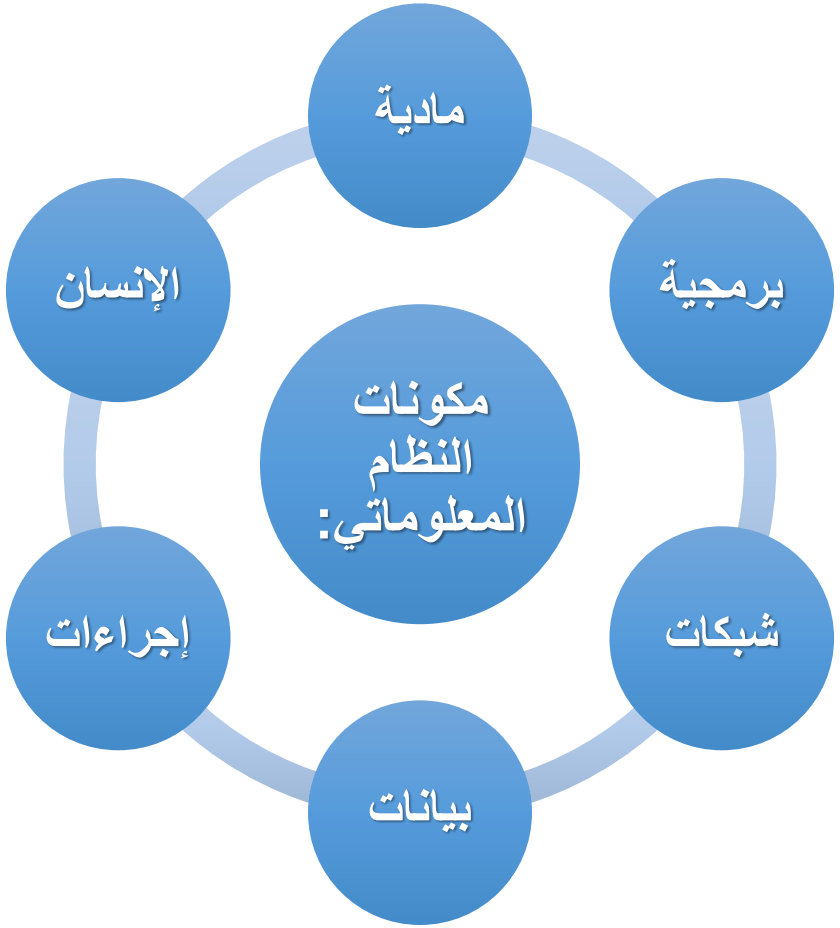
1 إلغاء تثبيت أو تعطيل برامج مكافحة الفيروسات؛ بسبب قيام المخترق بتعطيل هذه البرامج بهدف مساعدته على إخفاء أيّ تحذيرات قد تظهر على الجهاز.

2 إجراء الجهاز عدّة نشاطات من تلقاء نفسه، مثل تحرك مؤشر الماوس .

3 تغير كلمة مرور الجهاز: يدلّ تغيير كلمة المرور لتسجيل الدخول إلى الجهاز من تلقاء نفسها على اختراق الجهاز

4. زيادة نشاط الشبكة: تدلّ زيادة نشاط الشبكة، وتباطؤ سرعة الإنترنت على الاتصال بالجهاز عن بُعد

مكونات النظام المعلوماتي:



أنواع الجرائم المعلوماتية

إفشاء الأسرار: عن طريق الحاسب يمكن الاعتداء على خصوصيات الأفراد وإفشاء أسرارهم وذلك باستعمال بيانات شخصية حقيقية بدون ترخيص أو إفشاء أسرار بصورة غير قانونية وإساءة استعمالها أو عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عملية جمع ومعالجة ونشر البيانات الشخصية.

الابتزاز والتهديد: تهديد الجاني للمجني عليه إما بنشر أخباره أو صورة أو معلومات صحيحة ولكن لا يرغب المجني عليه لسبب ما ظهورها للآخرين وإما يهدده بنشر صور أو أخبار أو معلومات غير صحيحة ويقوم بطلب مقابل حتى لا ينشرها. مجرد فعل التهديد أو الابتزاز كاف لإقامة الحجة على هذه الجريمة.

جريمة التنصت: من يرتكب جريمة التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو التقاطه أو اعتراضه.

التشهير بالأشخاص: أصبحت هذه الجريمة من أبرز الجرائم الواقعة في الانترنت بل هناك مواقع صممت لأجل التشهير بالأشخاص

السطو على أموال البنوك: يتم ذلك عن طريق استخدام الجاني الحاسب الآلي للدخول إلى شبكة الإنترنت والوصول غير المشروع إلى البنوك والمصارف والمؤسسات المالية وتحويل الأموال من تلك الحسابات الخاصة بالعملاء إلى حسابات أخرى

التغرير: فيما يخص التغرير فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة حيث يوهم المجرمون ضحايا هذا النوع برغبتهم في تكوين صداقة على الانترنت.

البرامج الخبيثة

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:

1. الفيروسات (Viruses)
2. الديدان (Worms)
3. برامج التجسس (Spywares)
4. الخداع (Hoax)
5. عمليات الاحتيال واصطياد الضحايا The Phishing Scam
6. أحصنة طروادة Trojan Horses

أضرار الإصابة بالفيروسات و البرامج الخبيثة

1. تعطيل الحاسوب او التوقف المفاجئ له
2. بعض الأمور المزعجة للمستخدم مثل تغير سطح المكتب و حذف الملفات
3. تسرق البيانات
4. إتلاف البرمجيات و التسبب في الحرمان من استخدام بعض الخدمات
5. تبطئ الحاسب
6. تبطئ الاتصال بالانترنت

الفيروسات (virus)

- ماهو الفيروس:-
  - هو برنامج مكتوب باحد للغات الحاسب ويقوم باحداث اضرار فى الحاسب والمعلومات الموجودة على الحاسب وهو مصمم على ان يقوم باعدة كتابة نفسة على الملفات الموجودة على الحاسب او اى حاسب اخر يتم تبادل المعلومات بينه وبين الحاسب حامل الفيروس.
- من اين تاتى:-
  - من خلال الرسائل الالكترونية (مرفقات) - صفحات الانترنت
  - نسخ البرامج المقلدة - والأقراص القابلة للازالة
- ماهو التأثير:-
  - زيادة عدد العمليات حتى يتوقف الحاسب عن العمل
  - الغاء بعض ملفات النظام
  - اغلاق الحاسب من تلقاء نفسة
  - الغاء البرنامج المكتوب على الـ BIOS

ديدان الانترنت (worm)

- ماهى ديدان الانترنت :-
  - هى مثلها مثل الفيروس برنامج صغير مكتوب باحد للغات الحاسب مصمم على ان يقوم باعدة كتابة نفسة على الملفات الموجودة على الحاسب او اى حاسب اخر ولكنها متميزة بكونها ترسل نفسها منفردة الى قائمة البريد الالكترونى او الى كل جهاز بالشبكة وهى تنتشر بسرعة هائلة.
- من اين تاتى:-
  - من خلال الرسائل الالكترونية
  - نسخ البرامج المقلدة
  - صفحات الانترنت
  - الأقراص القابلة للإزالة
- ماهو التأثير:-
  - زيادة عدد العمليات حتى يتوقف الحاسب عن العمل
  - التحميل الزائد على الشبكة مما قد يبطئ العمل عليها تماما
  - احداث البطئ الشديد فى الانترنت

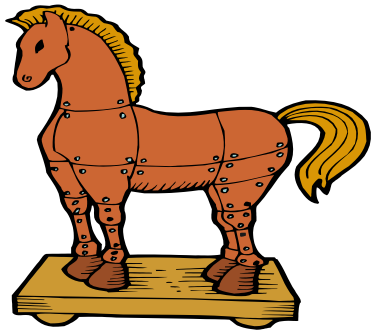
حواسيب الزومبي ZOMBIES

هي حواسيب مصابة بالفيروس، أو الودودة، أو حصان طروادة، متصلة بالانترنت أو تم اختراقها من قبل القراصنة، ويمكن أن تستخدم لأداء مهام خبيثة، عن طريق التصال عن بعد. وتستخدم أجهزة الزومبي كروبوت ضمن شبكة، غالبا ما تستخدم لنشر الرسائل الإكترونية غير المرغوب فيها وإطلاق هجمات حجب الخدمة، الاشخاص الذين تصاب أجهزتهم بالزومبي لا يدركون أنه يتم استخدام النظام الخاص بهم بهذه الطريقة، ويتم التحكم فيها عن بعد لأغراض خبيثة، أو أنشطة ضارة مثل تهكير كلمة السر، أو إرسال البريد اللكتروني غير المرغوب فيه.

نقاط WIFI واي فاي المخادعة

شبكات واي فاي المجانية متوفرة في كل مكان تق ريبا، ونقاط واي فاي المخادعة تقوم بتقليد هذه شبكات المجانية، هذه النقاط تعمل على مقربة من نقاط واي فاي الشرعية وتقدم عادة إشارات أقوى لخدع العديد من المستخدمين ليتصلوا بها، حالما يتم الاتصال بها تقوم بأخذ صورة عن جميع المعلومات التي يتم ارسالها من قبل المستخدمين للمواقع الشرعية والتي تتضمن أسماء المستخدمين وكلمات المرور.

احصنة طروادة (Trojan horse)



- ماهى احصنة طروادة:-
  - هو برنامج حاسوب موضوع فى احد البرامج التى تستخدم مثل الالعاب. تكسر الحماية المستخدمة لديك كما تتلف الملفات
- من اين تاتى:-
  - وهى تأتى غالبا مع الرسائل الالكترونية المرفق معها ملفات قابلة للتشغيل لذا لا تفتح أي ملف مرفق مع الرسائل الالكترونية.
  - وهى تأتى ايضا عند تحميلك للبرامج المجانية الموجودة على الانترنت لذا لا تحمل أي برنامج مجانى من الانترنت اذا كنت لا تعرف وتثق في الموقع الموجود عليه هذا البرنامج
- ماهو التأثير:-
  - يقوم بالغاء الملفات - يرسل رسائل مزيفة منك الى الموجودين فى قائمة البريد الالكترونى
  - كسر الحماية الخاصه بك

برامج التجسس (SPY Where & AD Where)

- ماهى :-

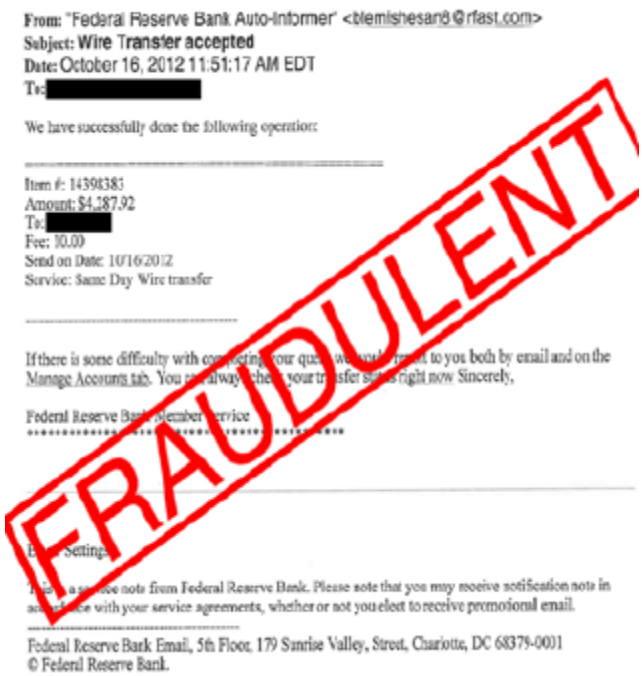
- برمجيات انتهاك الخصوصية او مجموعة من البرامج التى تقوم بتثبيت نفسها تلقائيا بمجرد الدخول على احد المواقع. هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة

- من اين تاتى:-
  - تصفح الانترنت "استخدام التطبيقات التى تستخدم تلك التكنولوجيا ".

- ماهو التأثير:-
  - ارسال معلومات خاصة بالمستخدم وطريقة استخدامة للانترنت.
  - معرفة ماهي المواقع الإلكترونية التي يقوم المستخدمون بزيارتها وما هي عادات وأساليب تصفح الإنترنت لديهم
  - فتح صفحات الانترنت الخاصة للجهة المصممة لهذا النوع "فتح صفحة عن اعلان لاحد المنتجات بمجرد دخولك على الانترنت"
  - إعادة توجيه مدخلات المتصفح لتوجه المستخدم إلى موقع آخرغير المقصود.

The Phishing Scam رسائل الاصطياد الخادعة

- التصيد هو محاولة الحصول على معلومات مثل أسماء المستخدمين وكلمات المرور وتفاصيل بطاقة الائتمان من قبل محتالين متنكرين بوصفهم أنهم يعملون في منظمات جديرة بالثقة.
- التصيد هي عملية يحتال فيها المهاجم حيث يرسل رسالة بالبريد الإلكتروني يطلب فيها بطاقات ائتمانية أو بطاقات التجارة الإلكترونية وتكون صالحة وسارية المفعول
- البريد الإلكتروني غالبا ما يستخدم أساليب التخويف في محاولة الإغراء الضحية إلى زيارة مواقع ويب مخادعة. يشعر فيها الضحية بانها مواقع عامة مثل التجارة الإلكترونية أو الخدمات المصرفية



الخدعة Hoax

- هو إنذار كاذب عن فيروس في الحاسوب. وعادة التحذير يصل عن طريق البريد الإلكتروني أو يتم توزيعها من خلال في الشبكة الداخلية للشركة
- فيروسات الخدعة، عادة ما تكون غير ضارة ولكنها تكون مزعجة باعتبارها خداع وتضيع للوقت وذلك من خلال إعادة توجيه الرسالة. و هناك عدد من الخداع من خلال تحذير المستخدمين أن ملفات النظام المهمة توجد بها فيروسات وبالتالي تقوم بتشجيع المستخدم عل حذف الملف، مما يسبب إتلاف النظام.
- كما انها تشكل حمل زائد على الشبكة و مساحة التخزين في سيرفر الميل

(Spam E-mail)

- ماهى :-
  - استقبال مجموعة من الرسائل الاكترونية "اعلانات" من عناوين وهمية متجددة فى كل مرة
- من اين تاتى:-
  - انتشار العنوان البريدى على الانترنت فى احد المواقع التى تم اختراقها واخذ كافة العناوين ووضعها قائمة الارسال او تباع من ISP او احد الشركات المسجل بها بيانات المستخدم.
- ماهو التأثير:-
  - استقبال رسائل غير مرغوب بها و إخفاء الرسائل المهمة في عدد كبير من الرسائل الغير مهمة.
  - شغل حيز من مصدر الانترنت المستخدم بالمؤسسة

نصائح عند فتح ملحقات البريد الإلكتروني

- لا تفتح أية ملفات ملحقة ببريد إلكتروني ما لم تعرف محتواها ومصدر.
- 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.
- تخصيص بريد خاص للاستخدامات الرسمية والهامة.
- تفادي الوقوع ضحية للرسائل الاحتيالية.

Social Engineering **الهندسة الاجتماعية**

- أو ما يعرف بفن اختراق العقول هي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو بكشف معلومات سرية بشكل إرادي. تُستخدم الهندسة الاجتماعية أحياناً ضمن احتيال الإنترنت لتحقيق الغرض المنشود من الضحية، حيث أن الهدف الأساسي للهندسة الاجتماعية هو طرح أسئلة (عن طريق الهاتف أو البريد الإلكتروني مع انتحال شخصية ذي سلطة أو ذات عمل يسمح له بطرح هذه الأسئلة دون إثارة الشبهات).

الأساليب المتبعة في الهندسة الاجتماعية

- من أشهر الأساليب المتبعة في مثل هذا النوع من الاختراق :
- الهاتف: فأكثر هجمات الهندسة الاجتماعية تقع عن طريق الهاتف . يتصل المهاجم مدعياً أنه شخص ذو منصب له صلاحيات و يقوم تدريجياُ بسحب المعلومات من الضحية.
- البحث في المهملات: حيث يوجد الكثير من المعلومات الهامة عن المنظمة يمكن الحصول عليها من سلة مهملات الشخص أو الضحية.
- الإقناع: حيث يحصل المهاجم على المعلومات التي يريدها من خلال التحدث مع الضحية وحثها على الإدلاء بمعلومات حساسة أو ذو علاقة بهدف المهاجم وذلك من خلال إثارة انطباع جيد لدى الضحية والتملق وغيرها من الأساليب.
- الهندسة الاجتماعية المعاكسة: وهي إيهام الضحية بأنك شخص مهم أو ذو صلاحيات عليا بحيث يقوم المهاجم بالإدلاء بمعلومات يريدها الضحية وإذا ما نجح الأمر وسارت الأمور كما خُطط لها فقد يحصل المهاجم على فرصة أكبر للحصول على معلومات ذات قيمة كبيرة من الضحية، وهذا الأسلوب معقد نسبياً كونه يعتمد على مدى التحضير المسبق وحجم المعلومات التي بحوزة المهاجم.

وسائل الحماية:

وسائل الحماية الفنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسئولياته.

من أمثلتها:

1. كلمة المرور.
2. القياس الحيوي.
3. التشفير.
4. الجدران النارية.
5. البرامج المضادة للفيروسات.
6. التوقيع الالكتروني.
7. توفير نسخ احتياطية (backup) .

استعادة السيطرة بعد اختراق الجهاز الشخصي

فصل جهازك من الإنترنت ليُفصل الرابط بينك وبين المخترق

إعادة تهيئة الجهاز

تثبيت برامج حماية الفايروسات وإجراء فحص شامل للجهاز

استعادة البيانات والمعلومات من النسخ الاحتياطية

نصائح عامة

1. لا تثقوا بأحد
2. حاولوا الحد من نشر المعلومات الشخصية
3. لا تقوموا بفتح المرفقات او الروابط
4. لا تقوموا باستخدام البرامج المقرصنة(المصدر هو الموقع المطور لها)
5. تأكدوا من تنصيب التحديثات(نظام التشغيل،برامج،مضاد فايروس،)لأغلاق الثغر الامنية
6. تأكدوا من تنصيب مضاد للفيروسات
7. استعملوا كلمات سر معقدة لا تستخدموا كلمة السر ذاتها في عدة حسابات
8. لا تخزنوا كلمات السر في المتصفح و تتأكدوا من تسجيل الخروج من حساباتكم وحذف الملفات المؤقتة و سجل التصفح عند نهاية كل جلسة او استخدموا التصفح الامن
9. لا تستخدموا هواتفكم الجوالة في تبادل المعلومات الحساسة ،تشفير الملفات ،إيقاف خدمة تحديد المواقع
10. استخدموا التشفير لملفاتكم الحساسة

وسائل الحماية

وسائل الحماية المادية

- ضع كمبيوترك وخصوصاً الكمبيوتر المحمول دائماً في مكان آمن.
- قم بحماية كمبيوترك بكلمة مرور ويستحسن أن تطفئه وأنت بعيداً عنه.
- عليك أن تشك في أي شخص يرغب في الحصول على أي من كلمات المرور الخاصة بك
- قم بانتظام بتغيير كلمة المرور
- لا تكتب كلمات المرور الخاصة بك في أي مكان ولكن عليك أن تتذكرها بنفسك.

وسائل الحماية

التحديثات

- ❖حافظ على تحديث جميع برامجك بما في ذلك أحدث نسخة من برنامج التشغيل الذي تستخدمه.
- ❖إذا كنت تستخدم التحديث التلقائي الذي يقوم بالبحث يومياً عن التحديثات عند بدء تشغيل الجهاز، فعليك إعادة تشغيل جهازك يومياً.

وسائل الحماية

جدار النار Firewall

❖يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين.

❖وتختلف جدران النار حسب احتياجات المستخدم.

❖علماً بأن الكثير من الشبكات والخوادم تأتي مع نظام جدار نار افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

قصة قصيرة

شكوى أعرابية إلى أحد الولاة في مصر، فقد جاءت
□أعرابية إلى قيس بن سعد فقالت له:
□أشكوا إليك قلّة الفئران في بيتي.
فما كان من ذلك الوالي إلا أن ملأ بيتها طعاما
□وكساء.

وسائل الحماية

التشفير

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات.

عندما ترسل المعلومات عبر الشبكة أو تخزن في الحاسب فإن إمكانية الوصول غير المصرح لها تكون موجودة، الحل يكون بالتشفير، وهو عملية ترميز المعلومات لجعلها غير مقروءة إلا من قبل الأشخاص الذين يملكون جزء منها يدعى مفتاح التشفير أو ببساطة، المفتاح.

لماذا نستخدم التشفير:

- لمنع الاطلاع على المعلومات المنتقلة عبر الشبكة
- استخدام بيانتك الشخصية لارسال رسائل مزيفة نيابة عنك
- التغير فى البيانات المنقولة عبر الشبكة
- تغير كلمات السر الخاصة.

انواع التشفير

التشفير المتماثل:

هو نوع من انواع التشفير والذى يحتوى على مفتاح للشفرة ونفس المفتاح لفك الشفرة.

التشفير غير المتماثل:

هذا النوع من التشفير والذى يحتوى على مفتاحين الأول لتشفير والاخر لفك الشفرة.

التوقيع الالكتروني

عبارة عن علامة أو برهان الكتروني يتم اضافته للملفات ، يتيح للمستخدم مستقبل الملف التأكد من أن الملف على صورته و شكله الاساسي و لم يتعرض للتعديل والتزييف.

يحتوي التوقيع الرقمي على قيمة خوارزمية فريدة تمثل بصمة خاصة للملف و يتم حساب هذه القيمة بالاعتماد على محتويات الملف، و من ثم يتم اضافة هذه القيمة للملف عند إرساله، و عند فتح الملف من قبل المستقبل يتم حساب القيمة مرة أخرى وفقا لمحتويات الملف فإذا اختلفت هذه القيمة يعني أن محتويات الملف قد تغيرت و يصبح الملف مزورا

كلمة المرور Password

مفاتيح للوصول الى ملفات او معلومات حساسة او محمية يمكن استعملها في حال ماسرقة في انتحال شخصيتكم او فتح حسابات ولا يمكن معرفتها الا بعد فوات الاوان

كلمة المرور Password

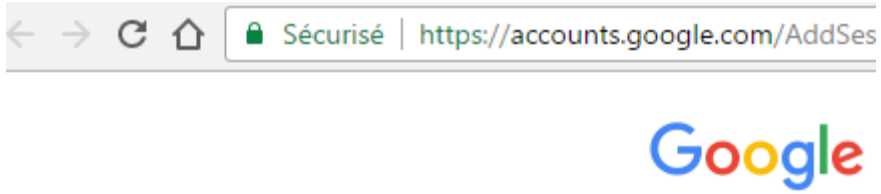
هي مجموعة من الرموز التي تسمح للدخول إلى الحاسوب، أو الموارد على شبكة الاتصال أو المعلومات.

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.

الطرق المثلى لاختيار و حفظ كلمات السر

1. عدم استخدام نفس كلمة المرور لعدة حسابات
2. أن تكون خاصة ولا يطلع عليها أحد مهما كان.
3. عدم كتابتها أبدا سواء كان في الجوال أو على ورق الملاحظات او تخزينها في الحاسوب.
4. يجب تغييرها كل شهرين كحد أقصى.
5. لا تستخدم نفس كلمة المرور في حسابات وأماكن أخرى.
6. لا تقبل أن يضع لك شخص أخر كلمة المرور.
7. عندما تشعر بأن أحد اكتشف كلمة المرور، قم بتغيرها فوراً.
8. عند إدخالك لكلمة المرور تأكد بأنه لا يوجد أحد يراقبك.
9. تجنب استخدام الحواسيب المشتركة مع الآخرين.
10. **https** تاكد من الروابط و شهادة الموقع



تعليمات اختيار كلمة المرور:

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

1. تجنبوا استخدام العبارات الشهيرة أو المستخدمة بكثرة في كلمات السّر
2. انشاء كلمة مرور يمكن تذكرها و يصعب تخمينها
3. تجنبوا استخدام معلومات شخصية(رقم الهاتف، أو اسم أحد الأقارب، أو تاريخ الميلاد)
4. كلمة مرور معقدة يُفضل أن تحتوي على أحرف وأرقام و الرموز الخاصة مثل ((*/-@+$)).
5. تجنبوا استخدام الأحرف المتجاورة مثلا تعتبر كلمة 123456 وأيضا qwertyمن أسوأ كلمات السرّ
6. يُفضل أن لا تقل عن 8 خانات.
7. يُفضل أن لا تكون مشهور ومتداولة(يجب أن لا تحتوي على اسم المستخدم).
8. يمكن استخدام معادلة بسيطة لإنشاء كلمة المرور
9. نضع حرف ، ثم الرقم الأول، ثم الرقم التالي يكون ثلاثة أضعاف الرقم السابق و هكذا.

	1*3=3				9*3=27		
A	1	#	3	W	9	$	7
			3*3=9				

Antivirus

- هناك العديد من انظمة الحماية من الفيروسات ومنها مايعمل بصورة فردية على الحاسبات الشخصية ومنها مايعمل فى بيئة الشبكات والاخير هام جدا فى المؤسسات التى بها عدد كبير من الاجهزة لما لها من خاصية السرفر والذى يتيح التحديث لكل الاجهزة مرة واحدة وكذلك التحذير المباشر لمسئول الشبكات عند دخول اى فيروس الى اى حاسب بالشبكة كما يتيح لمسئول الشبكات من عمل ازالة للفيروس من اى جهاز مصاب دون الانتقال الى الجهاز وبالتالى يسهل عملية التخلص من الفيروسات مباشرة.

KASPERSKY lab
ANTIVIRUS

AVIRA

sophos

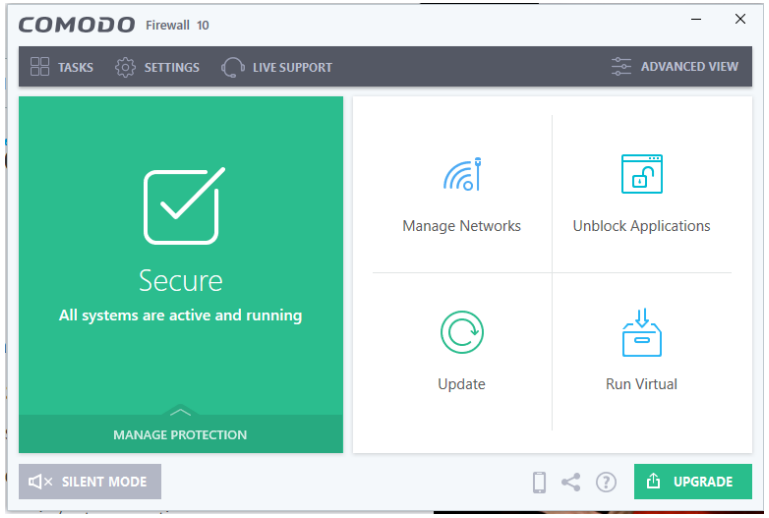
Antivirus USB

http://www.smadav.net

Firewall

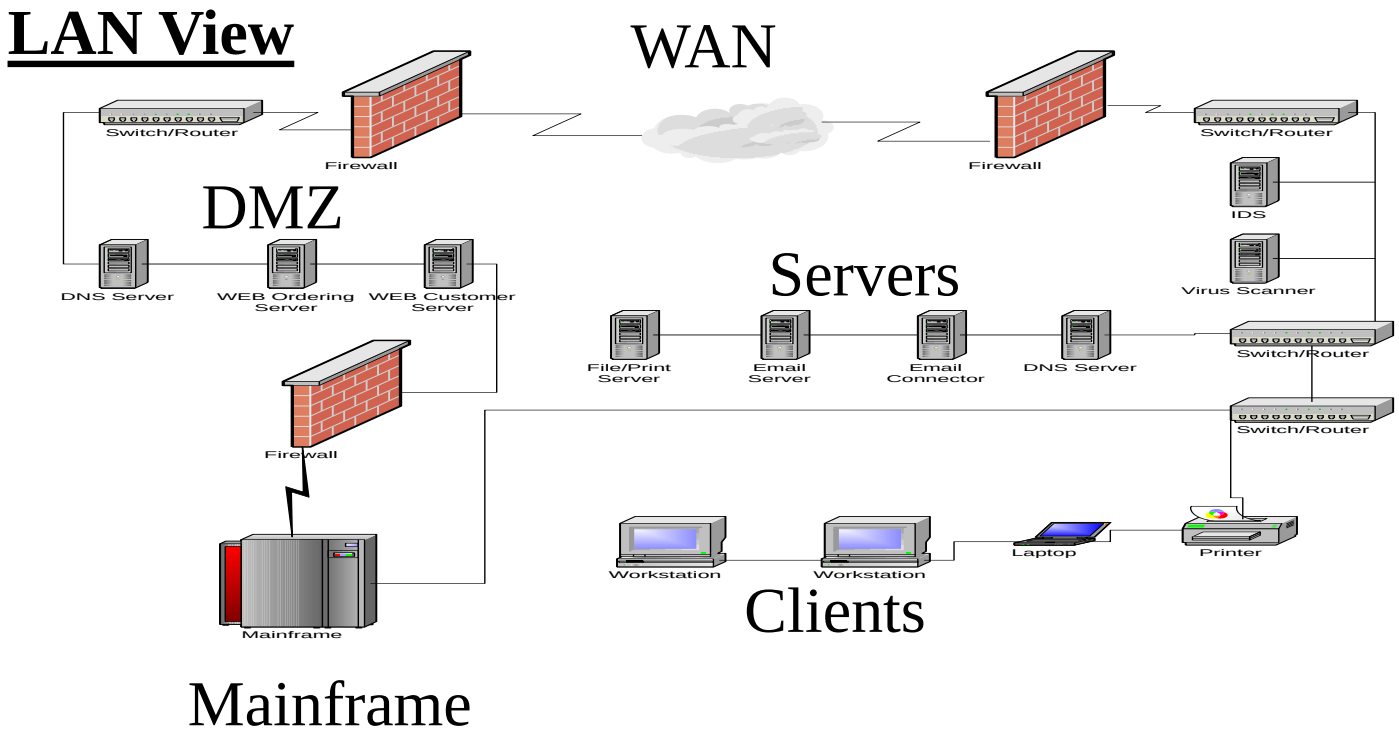
عبارة عن مجموعة من الاجهزة والبرامج التى تقوم بادارة تبادل البيانات بين شبكتين عبر الانترنت من خلال السماح او عدم السماح بالمرور الى الشبكة الداخلية.

COMODO
Creating Trust Online®



https://www.comodo.com

Firewall


LAN View
WAN
Switch/Router
Firewall
Firewall
Switch/Router
DMZ
IDS
Virus Scanner
DNS Server
WEB Ordering Server
WEB Customer Server
Servers
File/Print Server
Email Server
Email Connector
DNS Server
Switch/Router
Firewall
Switch/Router
Workstation
Workstation
Laptop
Printer
Clients
Mainframe
Mainframe

AntiLogger

- **Zemana AntiLogger**

حصل البرنامج على العديد من الجوائز العالمية , ومازال يحصد المزيد منها وذلك لمميزاته الجبارة , وسهولة استخدامه

مميزات البرنامج :

- **يستطيع تحذيرك عند قيام أحد البرامج بالتالي :**
- **محاولة التجسس على ضربات الكي بورد .**
- **محاولة التجسس على المايكروفون .**
- **محاولة التجسس على الكاميرا .**
- **محاولة التجسس على سطح المكتب بالتقاط صورة له .**
- **محاولة تعديل ملفات النظام .**

فحص الملفات على الانترنت

Virus Total

- **موقع مشهور جداً يتعامل مع أكثر من 40 مكافح فيروس مشهور في العالم , يتم فحص الملف المطلوب وإظهار النتيجة بدقة تقارب الفحص على الجهاز الشخصي , يرسل التقارير أول بأول لشركات الحماية والتي بدورها تحلل الملفات والبرامج**

https://www.virustotal.com

فحص الملفات على الانترنت

ThreatExpert :

- **http://www.threatexpert.com**
- **موقع للفحص أيضا , ويختلف عن سابقه بإعطائك تقرير مفصل عن نشاط البرنامج لو تم تشغيله على النظام , وما الذي سيحدث تحديداً . يجب التسجيل في الموقع**

فحص الملفات على الانترنت

- http://analysis.iseclab.org