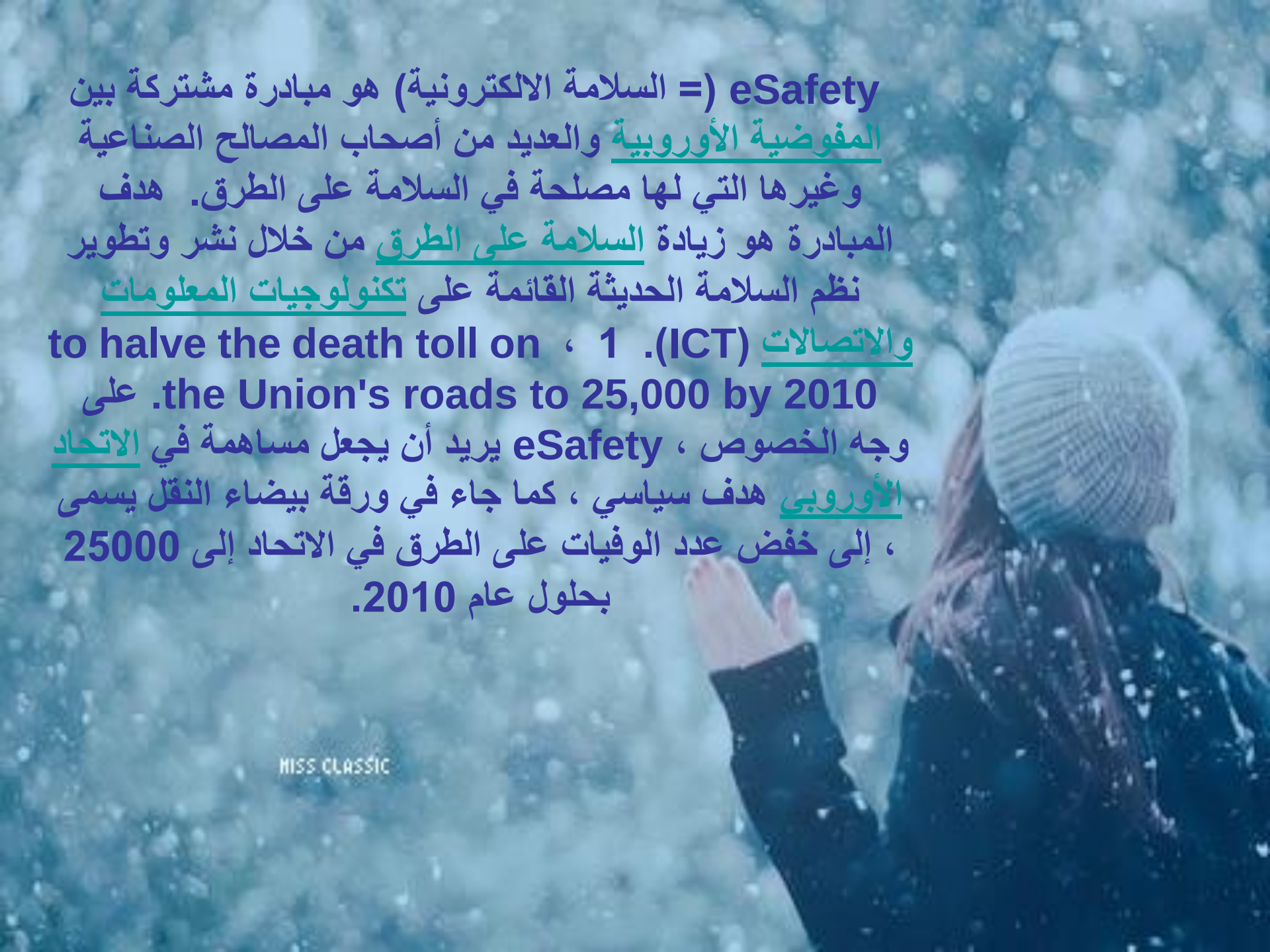
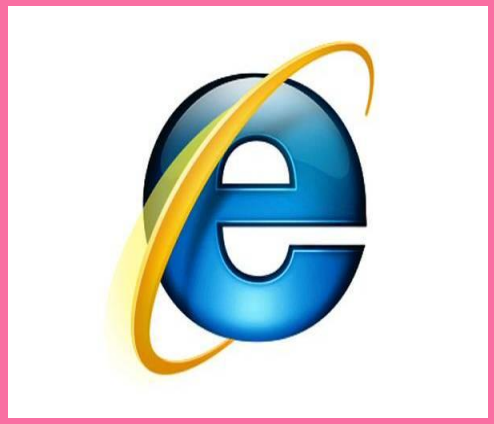
بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته

السلامه الإلكترونيه



eSafety (= السلامة الالكترونية) هو مبادرة مشتركة بين المفوضية الأوروبية والعديد من أصحاب المصالح الصناعية وغيرها التي لها مصلحة في السلامة على الطرق. هدف المبادرة هو زيادة السلامة على الطرق من خلال نشر وتطوير نظم السلامة الحديثة القائمة على تكنولوجيات المعلومات والاتصالات (ICT). 1 ، to halve the death toll on the Union's roads to 25,000 by 2010. على وجه الخصوص ، eSafety يريد أن يجعل مساهمة في الاتحاد الأوروبي هدف سياسي ، كما جاء في ورقة بيضاء النقل يسمى ، إلى خفض عدد الوفيات على الطرق في الاتحاد إلى 25000 بحلول عام 2010.



الأنترنت

سلاح ذو حدين، فهو مدخل للكثير من الأشياء النافعة، ولكن مع الأسف، فهو يفتح المجال أمام الكثير من الأشياء المؤذية للدخول إلى جهازك. وثمة العديد من المسائل الأمنية الواجب الاعتناء بها للإبقاء على سلاسة تشغيل أجهزة الكمبيوتر والشبكات. وسنناقش في هذا المقال أهم القضايا الأمنية وبعض الحلول لها.

كيف تحمي شبكتك ونظامك من الهكر؟!

عليك بالحذر والحرص الدائمين لحماية نظامك كي لا يكون عرضة للهجمات بسبب نقاط الضعف فيه، ويمكنك تركيب برامج فعالة لجعل استخدام الإنترنت أكثر أماناً لك.

البرامج التي تنصح بأستخدامها

1-Zonealarm with antivirus

2-TrendMicro Office Scan

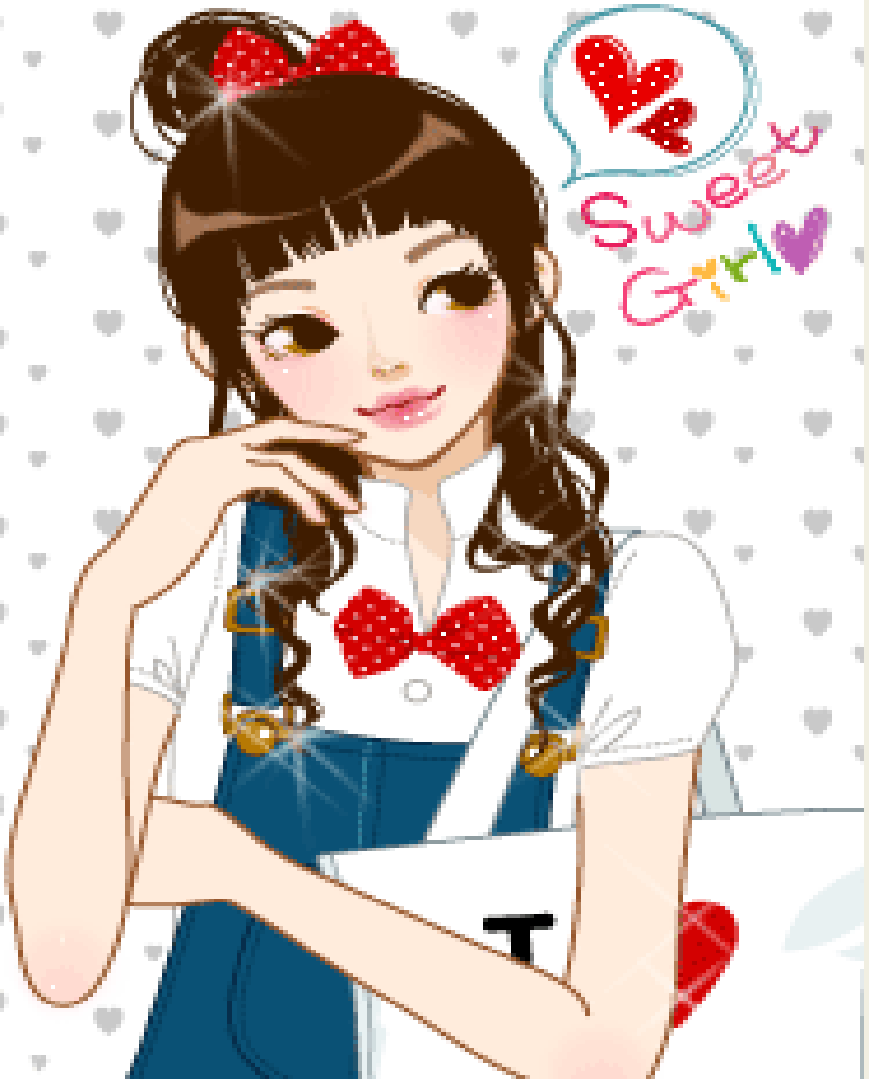
والاكثر استخداماً :-

جدار النار(Firewall)

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين.
وتختلف جدران النار حسب احتياجات المستخدم. فإذا استدعت الحاجة إلى وضع جدار النار على عقدة منفردة عاملة على شبكة واحدة فإن جدار النار الشخصي هو الخيار المناسب. وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار النار في الشبكة لتصفية جميع الحركة المرورية. 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.

طرق حماية جهاز الكمبيوتر من عبث الهاكر تتلخص في عدة أمور من أهمها يجب تركيب برنامج مكافح للفيروسات ساري المفعول (أي محدث) وعدم إضافة أي ملفات مرفقة غريبة تأتي عن طريق الإيميل ،وأيضا يفضل عدم تحميل أي برنامج من مواقع مشبوهة أو التسجيل فيها

كيف تحمي نفسك من الهاكر ؟



1.استخدم أحدث برامج الحماية من الهاكرز والفيروسات.

2.لا تدخل إلى المواقع المشبوهة: مثل المواقع التي تعلم التجسس أو المواقع التي تحوي أفلاماً وصوراً خليعة

3.عدم فتح أي رسالة إلكترونية من مصدر مجهول:

4.عدم استقبال أية ملفات أثناء (الشات) من أشخاص غير موثوق بهم: وخاصة إذا كانت هذه الملفات تحمل امتداد (exe) مثل (love.exe)

5.عدم الاحتفاظ بأية معلومات شخصية فى داخل جهازك: كالرسائل الخاصة أو الصور الفوتوغرافية أو الملفات المهمة وغيرها من معلومات بنكية مثل أرقام الحسابات أو البطاقات الائتمانية.

6.قم بوضع أرقام سرية على ملفاتك المهمة: حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط وهو أنت .

8.حاول دائماً تغيير كلمة السر بصورة دورية فهي قابلة للاختراق .

9.تأكد من رفع سلك التوصيل بالإنترنت بعد الإنتهاء من استخدام الإنترنت .

10.لا تقم بإستلام أي ملف وتحميله على القرص الصلب في جهازك الشخصي إن لم تكن متأكدا من مصدره .

11.الحرص على جعل كلمة السر ليست كلمة شهيرة و يفضل جعلها عديمة المعني و اضافة بعض الارقام و لا تقل عن 8 حروف مثل s4d3lt6v : او .. e4gol3s6 ووضع كلمة سر على الجهاز فهذه الكلمة حتى لو تمكن الهكر من وضع باتش على الجهاز فأن كلمة السر تمنعه من متابعة عمله .

12.ايقاف خاصية مشاركة الملفات -:

لـن يستطيع

وبهذه الطرق

الـ12

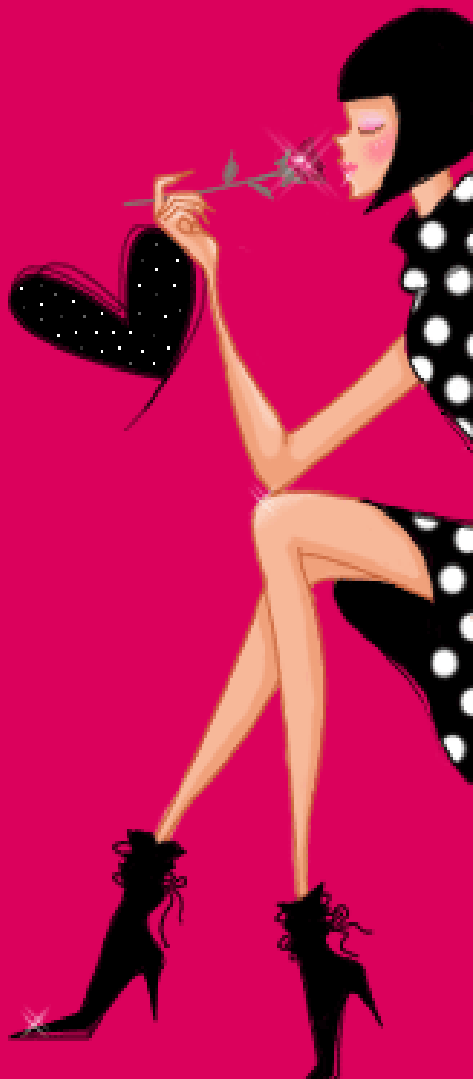
الـهاكر

اختراق

كمبيوترك الشخصي

التحديثات

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



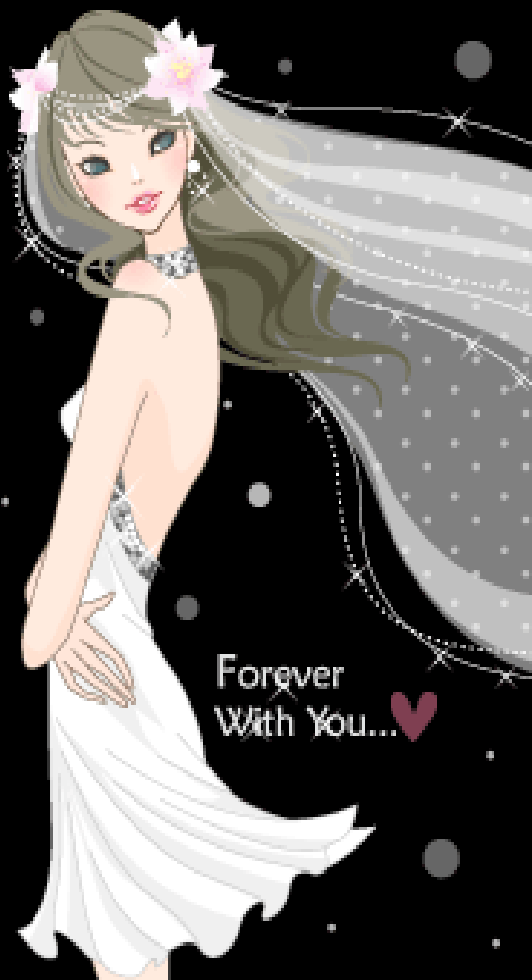
بعض النصائح :-

- 1 يجب على الفتاة أن لاتضع صورها على جهاز الكمبيوتر مهما كانت الأسباب فالمخترق عندما يخترق الجهاز يستطيع الحصول على جميع الصور في الجهاز بسهولة وتبدأ ماساة الأبتزاز وفضح الأعراض فلا تضعي اختي صورك أو أحدا من أهلك أو صور خاصة على الجهاز نهائيا مهما كانت الأسباب

-2عندما تشتري الفتاة جهاز كمبيوتر شخصي او محمول يجب ان تحرص كل الحرص أن لايكون فيه كميرا نهائيا فحتى لو كانت الكميرا مغلقة يستطيع الهكر ان يجعلها تعمل ويصور جميع من هم حول المحمول هي واخواتها وكل من يدخل الغرفة وحصلت مآسي كثيرة بهذه الغلطة الشنيعة

-3اذا كانت للفتاة صور او ملفات خاصة في سيدي أو فلاش ممري وارادت أن تشغلها في الكمبيوتر يجب عليها أن تفصل النت وتفصل الأتصال قبل ذلك فبمجرد دخول الفلاش ممري أو السيدي للجهاز اصبح جزءا من الجهاز واصبح اختراقه متاحا وسهلا فأحذري تمام الحذر

-4لاتستقبلي اي ايميل لاتعرفينه مهما كان فبفتحه يزرع الهكر تروجين في الجهاز مباشرة ويتحكم بجميع المنافذ والبورتات وتبدا الماساة



- 5لاتستقبلي ولاتضغطي على أي رابط او ملف لاتعرفينه الا بعد العرض على مواقع الفحص على النت أو برامج مكافحة الفايروسات والتاكد من خلوها من الفايروسات فالملفات المرسلة هي اسرع طريقة لأختراق أي جهاز بدون عناء

- 6يجب ان يكون المودم للأنترنت مشفر برقم سري ليس فقط الوايرلس بل ايضا الأتصال السلكي فيجب ان يكون الأتصال السلكي والاسلكي مشفر برقم سري فالهكر أذا تمكن من السيطرة على مداخل المودم تمكن من جميع مداخل الجهاز واصبح كانه صاحب الجهاز يمسح ويضيف مايشاء ويسجل ويدمر

-7لوكان لديكي بعض الصور سابقا في الجهاز ومسحتيها حتى لو حذفتيها يمكن إسترجاعها لذالك يجب الحذر من عامل الصيانة للأجهزة في محلات الكمبيوتر فباستطاعته أسترجاع جميع البيانات والصور من جهاز الكمبيوتر حتى بعد الفرمته لذلك أحرصي على ان لايصلح الجهاز الا من تثقين فيه ويكون اخوكي او والدك فوق راسه ومعه وهو يفرمت الجهاز أو يصلحه

- 8لو حدث وحصل أبتزاز لاقدر الله أتصلي بأقرب مركز هيئة واخبري أهلك مباشرة فالصبر على تعنيف الأهل أفضل من أن ترضخي للمبتز الذي سيفضحك ثم يهينك وبعدها ترجعين وتسنتجدين بأهلك بعدما ضاع الشرف والعفة فأبدأي باهلك مباشرة ولاتخافي فمهما قسوا عليك فأنت ابنتهم ودمهم ولحمهم أما المبتز فهو نجس قذر سيريكي الذل والفضيحة وستندمين أشد الندم

عمل الطالبه :-

ظبيه المري

الصف :-

أول ثانوي