حلم الجميع على مر العصور كان الأمن الكامل ، وهذه الحالة لا يمكن أن تصل إليها و أنت تمتلك حاسباً تدرك تمام الإدراك أنه قد يكون هناك من يتجسس عليك ، و يتابع تحركاتك .

فأنت أو غيرك كالشخص الذي يعلم أن هناك ثغرة في جداره تمكن جاره من مشاهدته وهو في بيته ، فهل ستستطيع حينها الشعور بالأمان .. !!

الاختراق اليومية والتي تتم بواسطة أطفال الهاكرز الذين لوثوا الإنترنت بجرثوماتهم ، و للأسف أصبحوا لا يفرقوا بين أحد

أصبحوا يستهدفوا حتى المنتديات و المواقع الإسلامية و يجربوا آلاف الأكواد الضارة و التي تصنف على أنها من أخطر الفيروسات ، هذا بالإضافة إلى تتبع عورات المسلمين ، و فضحهم عبر مواقع هدفها الأول و الأخير (كشف المستور) و الذي يتفاخر به القاصي و الداني هنا أو هناك .

لذا كان من الواجب أن نعرف الطرق الكفيلة بإغلاق أي باب قد يستخدمه أي أحد للتجسس علينا

و بإذن الله فور قراءتك وتطبيقك لما جاء في الشرح ستكون قادر على إدارة جهازك بشكل كامل و التخلي عن محلات الصيانة البرمجية لجهازك ، هذا بالإضافة إلى القدرة الكاملة في حماية نفسك بنسبة 100% ..


بين كل فترة وأخرى نسمع عن هجمات
الفيروسات ومدى الدمار الذي تسببه.
كمان سمع عن تسلل أحد المتطفلين إلى
قاعدة معلومات عسكرية ومنشآت
حكومية. إضافة إلى مجرمي التقنية
الحديثة الذين يستخدمون أرقام بطاقات
الائتمان بعد رصدها من شبكة الإنترنت
وأبعد اختراقهم لأجهزة بعض
المستخدمين

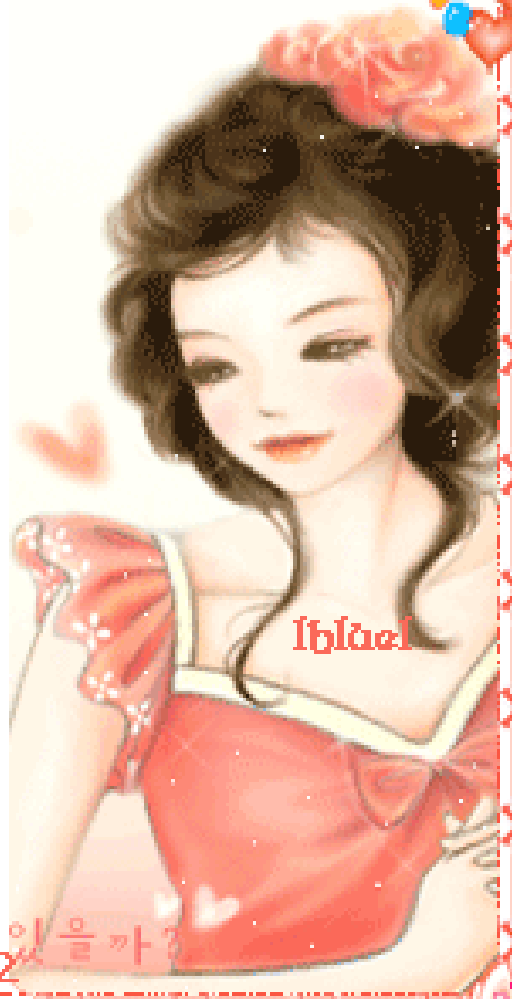
فضلا عن هؤلاء الذين يتسللون إلى شبكات البنوك والشركات الكبرى!
وكل ذلك بسبب عدم الأخذ بأسس وقواعد الأمن ولضعف الإجراءات الأمنية المتخذة. وقد نتج عن ذلك خسائر تقدر بمئات الملايين ولكن الأمور الآن أصبحت أكثر صرامة وصعوبة أمام المخترقين والمتطفلين خاصة بعد سن القوانين التي تجرم من يقوم بتلك الأفعال وتطور مستوى البحث والتحري لتتبع أثر المجرمين على الشبكة.

كما لا ننسى أنها أيضا نتيجة مباشرة لزيادة الوعي لدى الشركات والبنوك بأهمية الأمن ولذلك فإن هؤلاء المتطفلين والمجرمين بدؤوا بالبحث عن مستخدمين عاديين. كما أن هناك فئة مريضة بحب التطفل والتجسس على الناس. كذلك هناك مجرمون ممن يريدون إرسال تهديد أو فيروسات فيقومون باستخدام جهازك دون علمك وقبل أن تشعر بهم ومن ثم يضعوك أنت في وجه المدفع أمام الجهات الرسمية. وهذا احصل قبل عدة أشهر عندما قام بعض الأشخاص بتعطيل أشهر المواقع الأمريكية مثل ياهوو وأمازون دوت كوم وذلك بتسخير مئات من الكمبيوترات الخاصة بالجامعات وبعض الشركات والأفراد لإرسال كميات هائلة من المعلومات والطلبات حتى تعطلت المواقع وشلت الحركة بها تماما أمام المستخدمين وتسبب في خسائر تقدر بمئات الملايين من الدولارات.

هناك عديد من مصادر التهديد الأمني لمستخدمي شبكة الإنترنت.تأتي الفيروسات في المرتبة الأولى ومن ثم تليها كل من أحصنة طروادة وديدان الإنترنت. والاختراق (سواء كان اختراقاً لشبكة حاسب أوجهاز شخصي) وتعرف ب«الهاكينج». والجافاسكريبت والجافا أبليت والأكتاف اكس. وجواسيس البريد الإلكتروني. وراصدي لوحة المفاتيح. إضافة إلى مصادر تهديد للخصوصية والتي قد تهدد الأمن مثل: كعكة الإنترنت أومأ يعرف بالكوكيز.
ومصادر متعلقة بالبريد الإلكتروني مثل المحولين (رفيرر) ومرسلي الرسائل الإلكترونية الإزعاجية (سبامرز) وغيرهم.
الفيروسات

هي برامج صغيرة تصيب الأجهزة وتتسبب في الكثير من المشاكل الخطيرة كمسح الذاكرة الصلبة ومسح بعض الملفات الهامة في أنظمة التشغيل والقيام بإصدار الأوامر لبعض البرامج دون علمك وأتدخل مباشر منك مثل ما عمل فيروس الحب.
ولمزيد من المعلومات عن أنواع الفيروسات وكيفية عمل البرامج المضادة يمكن الإطلاع على التفاصيل المتوفرة في موقع شركات برنامج الحماية من الفيروسات مثل نورتن ومكافئي وغيرها.

وتعتبر الرسائل الإلكترونية أكبر مصدر للفيروسات وذلك لسهولة إضافتها كملفات ملحقة وسرعة انتشارها على الشبكة في زمن قصير جدا. وتعتبر نسخ البرامج المقلدة مصدرا آخر للفيروسات. أما المصدر الأقل انتشارا فهو الأقراص اللينة ولكنها أخطر بكثير من المصادر الأخرى وذلك لتعاملها المباشر مع نظام بدء التشغيل لجهازك.
أما أحصنة طروادة وديدان الإنترنت فهي شبيهة جدا بالفيروسات ولكنها تختلف في الهدف. فمثلا الديدان تقوم بمسح أو تدمير المعلومات من البرامج التطبيقية كبرامج المحاسبة وقواعد المعلومات فقط كما أن بمقدور هذه الديدان التكاثر حتى تملأ الذاكرة وتعطل الجهاز الضحية. أما أحصنة طروادة فهي لا تدمر ولاتمسح المعلومات ولكنها تتجسس وتقوم بجمع المعلومات والبيانات ومن ثم إرسالها لمصدرها (مرسل برنامج حصان طروادة) والذي غالبا ما يكون فرداً أوموقعاً أومنظمة لجمع المعلومات.

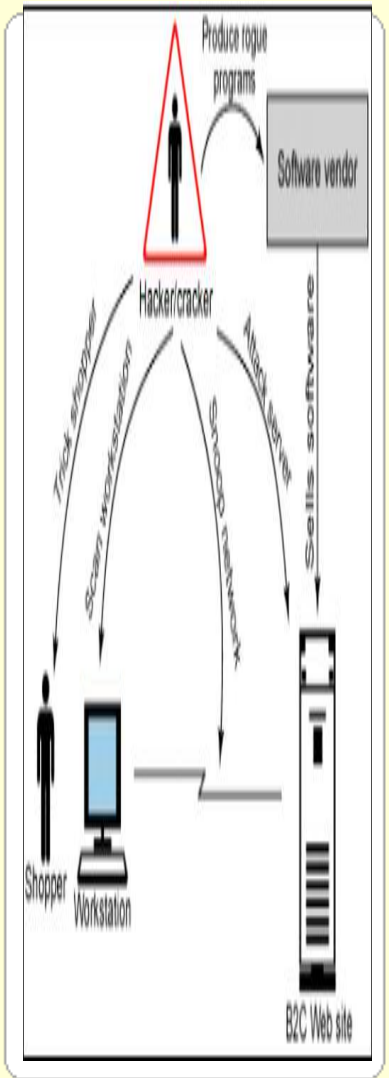


الاختراق

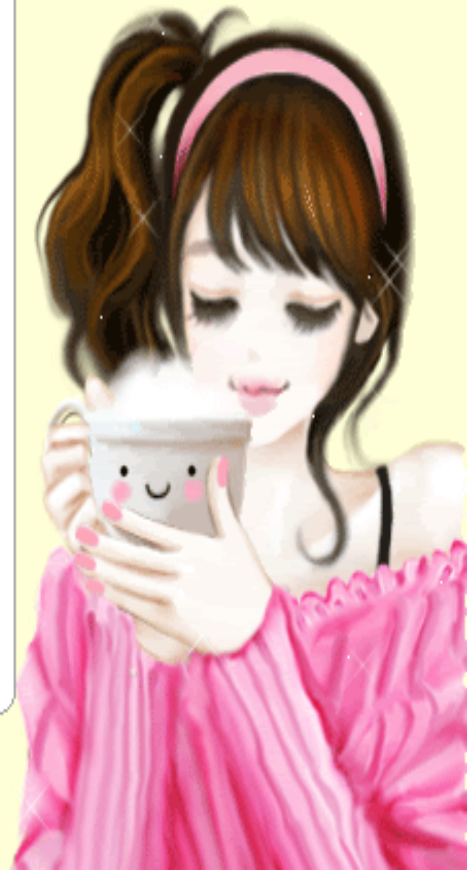
ويعني قيام أحد الأشخاص الخبراء بالتعامل مع الكمبيوتر والإنترنت بمحاولة الوصول إلى جهازك والشبكة الخاصة بشركتك عن طريق شبكة الإنترنت وذلك باستخدام برامج متخصصة في فك الرموز والكلمات السرية وكسر الحواجز الأمنية واستكشاف مواطن الضعف في جهازك أوشيكة معلوماتك.

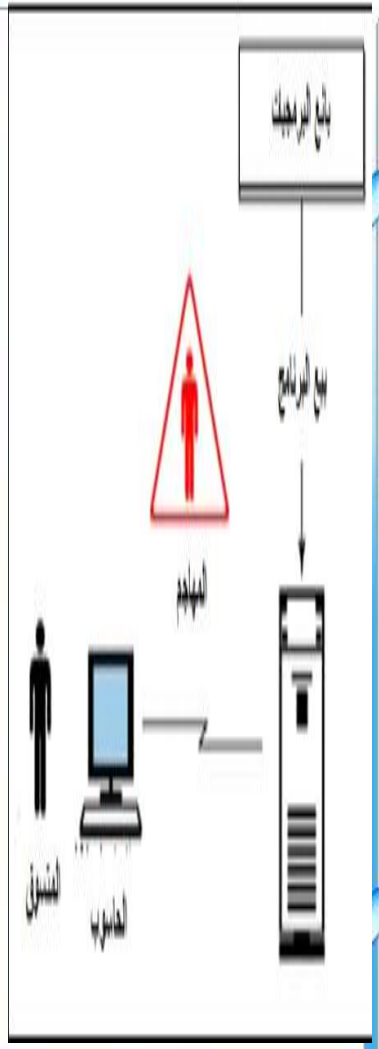
وعادة ما تكون المخارج (بوابات العبور للمعلومات) الخاصة بالشبكة المحلية. وهذه أسهل الطرق للوصول إلى جميع ملفاتك وبرامجك. وبالنسبة للمخترقين أصبحت المهمة عسيرة بعض الشيء لاختراق المؤسسات والمواقع الكبيرة بعد تطور نظم الدفاع وبرامج الحماية. ولكن بالنسبة لأجهزة الأفراد مازالت الأبواب مفتوحة.

تقنيات حديثة



جافا سكري بت وجافا أبليت والأكتاف أكس وكلها تقنيات حديثة ومفيدة ولكن تهدد أمن المستخدمين علما بأن الأخيرتين تعتبران أساسا من الأدوات المهمة جدا لتصميم المواقع الحديثة. غير أن سوء استخدام هذه التكنولوجيا يهدد مستقبلها ومدى انتشار شعبيتها. وذلك لقيام العديد من المستخدمين المتمرسين بتعطيل هذه الخاصية من المتصفح الخاص بها وبالتالي العزوف عن المواقع المصممة على أساس هذه التكنولوجيا مما يؤدي إلى فقدان شريحة كبيرة من المستخدمين لأنها مصدر خطير جدا على الأمن. وعادة تقوم المواقع المشبوهة والعائدة ملكيتها لأحد المحتالين باستخدام هذه التقنية بكثرة لأنها قادرة على رصد كلمات السر والعبور وكذلك تدمير وتعديل الملفات المخزنة أملفات البرامج.

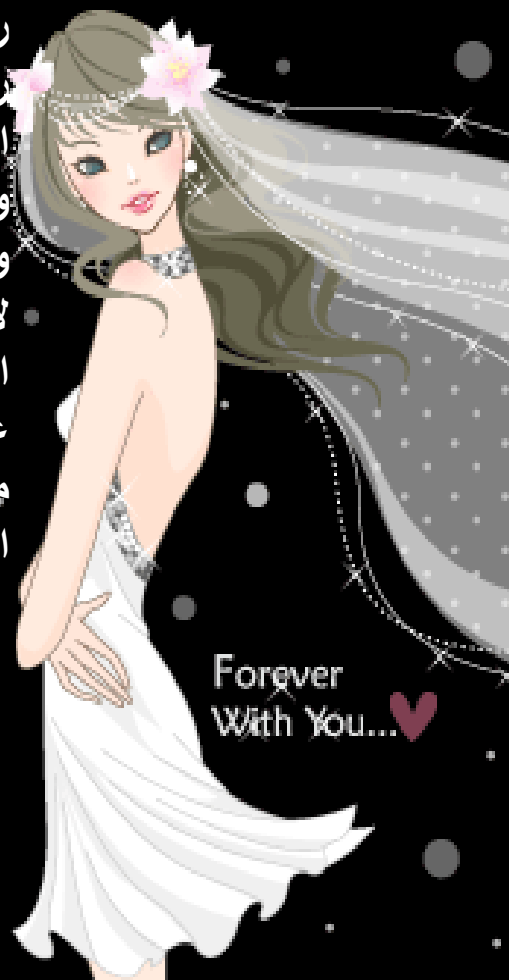




ولهذا السبب تتجنب معظم المواقع العالمية الإفراط فيها بينما يقوم أصحاب المواقع الشخصية باستخدامها بكثرة.
جواسيس البريد الإلكتروني عادة من المخترقين السابقين لجهازك أومن يشاركونك الجهاز فعليا سواء في المنزل والعمل. أو مستخدم آخر للجهاز خاصة إذا كنت في مقهى للإنترنت ولم تخرج من برنامج البريد بشكل صحيح أولم تقم بالخروج من برنامج المتصفح.

وهم من أخطر مصادر التهديد الأمني حيث إنهم قادرون على رصد أي ضغطة على لوحة المفاتيح وبذلك يتمكنون من رصد كل ما يتم كتابته على لوحة المفاتيح خاصة اسم المستخدم وكلمات العبور وذلك حتى قبل أن يتمكن جهازك وبرنامجك من إخفاء وتشفير الكلمة

ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة لأنها تتطلب الوصول إلى جهازك فعليا. ويكثر استخدام هذه البرامج من قبل النساء (الزوجات) لمراقبة دردشة الأزواج على الشبكة ! كما يستخدمها بعض ضعاف النفوس لرصد معلومات الغير في مقاهي الإنترنت والأجهزة العامة في المكتبات وغيرها من الأماكن الأخرى.



ثانيا: المزعجون:

وهي عادة الشركات والمواقع التي تحصل على عنوان بريدك الإلكتروني وتقوم بتبادل هذه العناوين فيما بينها أو تقوم ببيع هذه العناوين وكذلك يقوم بعض الأفراد بجمع هذه العناوين للقيام بإزعاج الآخرين ألغرض بيعها لإحدى الشركات. وقد انتشرت مؤخرا رسائل باللغة العربية تحكي قصص محزنة لأطفال وكبار تعرضوا لحوادث شخصية أحوادث سير (طبعا كلها من نسج الخيال) ويطلب منك صاحب الرسالة بأن تساعد ذلك الطفل المسكين بارسال الرسالة الى كل من تعرف ومن لا تعرف!! وطبعا أنت من ذوي القلوب الرحيمة والطيبة فتقوم بالعمل نيابة عنه بينما يقوم هو بجمع العناوين وتكوين ثروة من العناوين يقوم ببيعها أو يكون قد أرسل معها فيروسا أوبرنا مج تجسس أو برنامج للتحكم وتعطيل المواقع وأنت لأتعلم عنها.

كما انتشرت في الآونة الأخيرة رسالة تحتوي على معلومات عن أحد مكونات الشامبو وأنها تسبب السرطان.

ويذكر فيها منتجا معينا ويمدح فيه بينما يذم في بقية الأنواع. ويطلب منك إخبار كل الأصدقاء والمعارف عن طريق تحويل الرسالة. وطبعا كل هذا الكلام ليس له أساس من الصحة والهدف منه جمع العناوين أو التسويق للشامبو الخاص بهم.

وللوقاية والحماية أثناء استخدام البريد الإلكتروني يجب إتباع الآتي:
استخدام برامج مضادة للفيروسات وبرامج حماية وبرامج التشفير المتخصص.
استخدام كلمات عبور سهلة التذكر ولكن صعبة التخمين كأن تكون مكونة من حروف وأرقام أخليط من الأحرف الكبيرة والصغيرة.
غلق المتصفح حال ابتعادك عن الجهاز لتعطيل خاصية الرجوع للخلف في المتصفح.
عدم استخدام خاصية تذكر اسم المستخدم وكلمة العبور.
عدم استخدام خاصية الإكمال الآلي والتلقائي للاسم وفراغات النماذج في المتصفح.
عدم استخدام خاصية تذكر الصفحات التي تقوم بزيارتها لفترات طويلة وتقليل هذه المدة على قدر المستطاع.
عدم فتح الملفات المرفقة إذا كانت من أحد الأنواع التي تم ذكرها في البداية.
عدم تحويل الرسائل المشبوهة إلى أصدقائك ومعارفك.
تعديل خاصية الأمن في المتصفح إلى المستوى المتوسط والأعلى مع تعطيل خاصية الجاف سكري بت. وتعديل مستوى الأمن في خاصية الأكتاف أكس.
عند الانتهاء من قراءة الرسائل عليك بالخروج بطريقة صحيحة من الموقع والبرنامج ويكون ذلك بتسجيل الخروج أومايعرف ب Sign out. لأن هنالك بعض برامج البريد والمواقع تتذكرك لمدة تصل إلى 8 ساعات وترحب بك مباشرة حال دخول أي شخص آخر للموقع ذاته

وهم من أخطر مصادر التهديد الأمني حيث إنهم قادرون على رصد أي ضغطة على لوحة المفاتيح وبذلك يتمكنون من رصد كل ما يتم كتابته على لوحة المفاتيح خاصة اسم المستخدم وكلمات العبور وذلك حتى قبل أن يتمكن جهازك وبرنامجك من إخفاء وتشفير الكلمة

ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة لأنها تتطلب الوصول إلى جهازك فعليا. ويكثر استخدام هذه البرامج من قبل النساء (الزوجات) لمراقبة دردشة الأزواج على الشبكة ! كما يستخدمها بعض ضعاف النفوس لرصد معلومات الغير في مقاهي الإنترنت والأجهزة العامة في المكتبات وغيرها من الأماكن الأخرى.