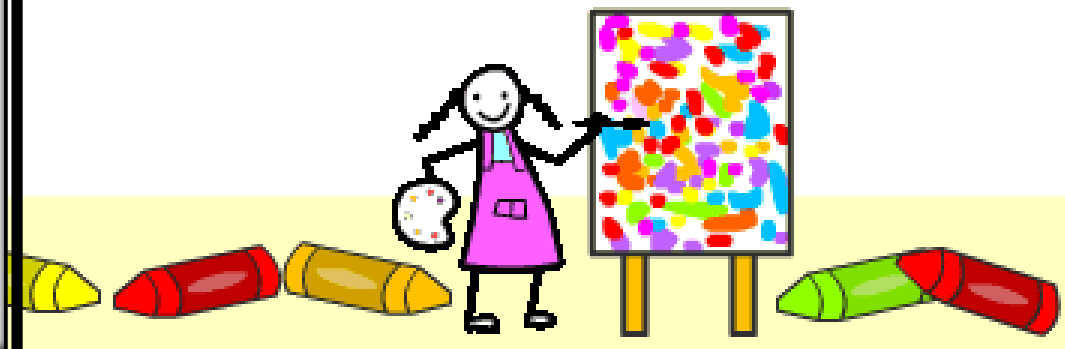

الأمن الإلكتروني
Parisnajd.co

بين كل فترة وأخرى نسمع عن هجمات الفيروسات ومدى الدمار الذي تسببه. كمانسمع عن تسلل أحد المتطفلين إلى قاعدة معلومات عسكرية أومنشآت حكومية. إضافة إلى مجرمي التقنية الحديثة الذين يستخدمون أرقام بطاقات الائتمان بعد رصدها من شبكة الإنترنت أوبعد اختراقهم لأجهزة بعض المستخدمين. فضلا عن هؤلاء الذين يتسللون إلى شبكات البنوك والشركات الكبرى!
وكل ذلك بسبب عدم الأخذ بأسس وقواعد الأمن أولضعف 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 ارسال تهديد أو فيروسات فيقومون باستخدام جهازك دون علمك وقبل أن تشعر بهم ومن ثم يضعوك أنت في وجه المدفع أمام الجهات الرسمية. وهذا ماحصل 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 لارسال 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 ابليت والأكتف إكس. وجواسيس البريد الإلكتروني. وراصدي لوحة المفاتيح. إضافة إلى مصادر تهديد للخصوصية والتي قد تهدد الأمن مثل: كعكة الإنترنت أوما 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 أومسح بعض الملفات الهامة في أنظمة التشغيل أوالقيام بإصدار الأوامر لبعض البرامج دون علمك أوتدخل مباشر منك مثل ما عمل فيروس الحب. ولمزيد من المعلومات عن أنواع الفيروسات وكيفية عمل البرامج المضادة يمكن الاطلاع على التفاصيل المتوفرة في موقع شركات برنامج الحماية من الفيروسات مثل نورتن ومكافي 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 برامج التطبيقية كبرامج المحاسبة وقواعد ما أن بمقدور هذه الديدان التكاثرحتى تملأ الجهاز الضحية. أما أحصنة طروادة فهي لا تدمر ت ولكنها تتجسس وتقوم بجمع المعلومات م إرسالها لمصدرها (مرسل برنامج حصان البا ما يكون فرداً أوموقعاً أومنظمة لجمع

الاختراق

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

بوابات العبور للمعلومات) الخاصة بالشبكة) وعادة ما تكون المخارج 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 سكريبت وجافا أبليتس والأكتف إكس 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 الى فقدان شريحة كبيرة من المستخدمين لأنها مصدر خطير جدا على الأمن. وعادة تقوم المواقع المشبوهه والعائدة ملكيتها لأحد المحتالين باستخدام هذه التقنية بكثرة لأنها قادرة على رصد كلمات السر والعبور وكذلك تدمير وتعديل الملفات المخزنة أوملفات البرامج.

ولهذا السبب تتجنب معظم المواقع العالمية الإفراط فيها بينما يقوم أصحاب المواقع الشخصية باستخدامها بكثرة.

جواسيس البريد الإلكتروني

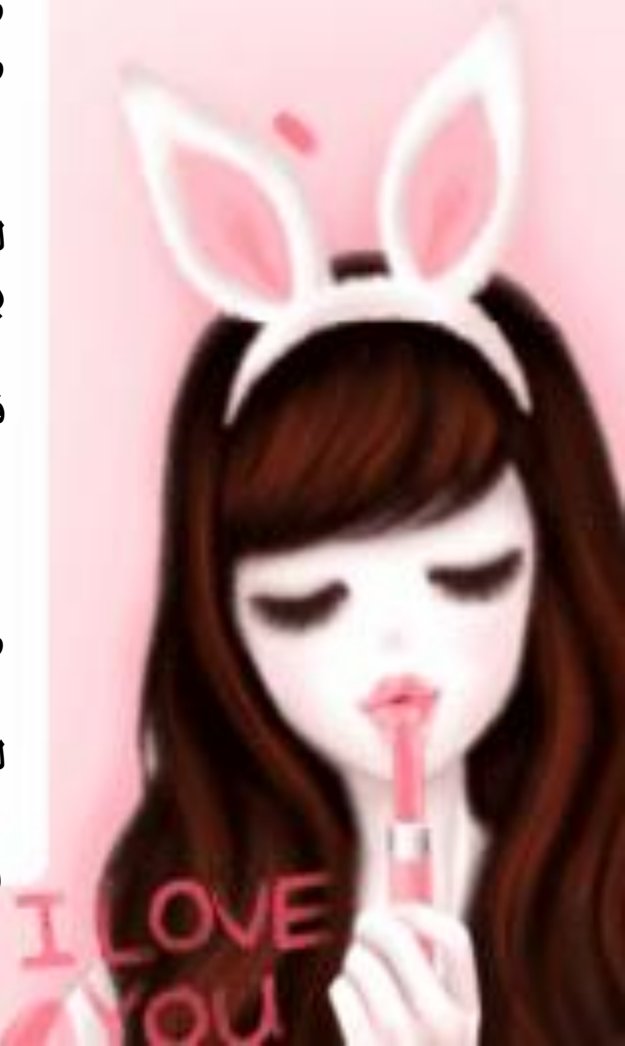
وهم عادة من المخترقين السابقين لجهازك أوممن يشاركونك الجهاز فعليا سواء في المنزل أوالعمل. أو مستخدم آخر للجهاز خاصة إذا كنت في مقهى للإنترنت ولم تخرج من برنامج البريد بشكل صحيح أولم تقم بالخروج من برنامج المتصفح.

راصدو لوحة المفاتيح

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 أوبرنامجك من اخفاء وتشفير الكلمة
ولحسن الحظ فإن هذه البرامج غير منتشرة عبر الشبكة ويكثر استخدام .لأنها تتطلب الوصول الى جهازك فعليا 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 الاماكن الأخرى. ولذلك يتردد الكثير من المستخدمين ممن يعتمدون على الأجهزة العامة كمقاهي الإنترنت (ولا يمتلكون أجهزة خاصة بهم) من الشراء المباشر من الإنترنت واستخدام بطاقات الائتمان ويفضلون التحويل البنكي أوالاتصال لإملاء الرقم بالهاتف أما إذا كنت تتسوق من جهازك الخاص فلا داعي للقلق.

خطوات وإجراءات بسيطة

هنالك عدة إجراءات بسيطة ينبغي التعود عليها أثناء تصفحك للإنترنت. علما بأن هذه الإجراءات لا تغنيك عن اقتناء برنامج حماية متخصص ولكنها كافية لكي تبدأ ببناء خط دفاعي أول وقوي يصعب من مهمة اللصوص والمتطفلين خاصة اذا كنت تعمل من جهاز شخصي متصل بالإنترنت عن طريق مودم. أما إذا كنت متصلاً بالإنترنت بطريقة أسرع كالخطوط الرقمية فأنت بحاجة فورية لبرنامج متخصص للحماية والسبب هو حصولك على رقم أي بي (عنوان بروتوكول الإنترنت) ثابت مخصص لك. ما يسهل عملية تتبعك على الإنترنت. أما لوكنت تستخدم فاكس مودم عاديا للاتصال بالإنترنت فإن مزود الخدمة لا يخصص لك رقم أي بي محددا ولكنك تحصل على رقم مختلف كلما قمت بالاتصال على الشبكة. أما لوكنت تملك شبكة من الكمبيوترات المتصلة مع بعضها البعض وجهازك يعتبر جزءا من هذه الشبكة المتصلة بالإنترنت فإنك بحاجة فورية لبرنامج حماية متخصص (جدران اللهب) وذلك لأن المخارج المخصصة لمشاركة الملفات تكون مفتوحة وجاهزة ومواتيه لدخول الهاكر.



نصائح

احصل على نسخة أصلية وحديثة من نظام التشغيل لأنه هوأساس الحماية وفي نفس الوقت يمكن أن يكون أكبر نقطة ضعف في جهازك. وفي الحقيقة تقوم الشركات المنتجة لأنظمة التشغيل بتحديث وتعديل هذه الأنظمة كلما يتم اكتشاف خلل أمني. وعادة يتم إخبارك بالبريد الإلكتروني أوبطريقة مباشرة من خلال ارتباطك المباشر بالشركة المنتجة أوزيارة موقع الشركة والبحث عن التحديثات ومن ثم تنزيل الملفات الخاصة بالتحسينات على نظام التشغيل. وعادة لا يتمتع من يملك نسخة مقلدة بهذه الميزة.

قم بتنزيل أحدث نسخة من المتصفح. وذلك لأن الإصدارات القديمة تتخللها العديدمن الثقوب الأمنية والتي تجعل منك هدفا سهلا. وطبعا إذا كنت ممن يشترون من خلال الشبكة احصل على نسخة مدعومة بقوة تشفير 128 بت. كما ينصح بتعديل مستوى الأمن في المتصفح وذلك بمنع وتعطيل التشغيل المباشر لأكتف إكس وجافا وجافاسكريبت.

إذا كنت تملك نظام تشغيل LAN: التحكم بملفات الشبكة المحلية ويندوز ولست متصلا بشبكة حاسبات آلية داخل المكتب اوالمنزل. أي انك لست بحاجة إلى أي نوع من أنواع الملفات الخاصة بالمشاركة. قم بمسح وإزالة أي نوع من ملفات المشاركة لأن نظام ويندوز يقوم بفتح هذه الملفات بطريقة مباشرة كشيء أساسي في النظام. وتعتبر هذه الملفات أكبر مصدر تهديد أمني لك لأنها تسمح لأي شخص في الإنترنت من الدخول إلى جهازك ومشاركتك في ملفاتك ومعلوماتك الموجودة في الجهاز.

احم جهازك بكلمة مرور تمنع الآخرين من الدخول إليه. فهناك عدة كلمات عبوريمكنك إنشاؤها في جهازك، فمثلا يمكنك وضع كلمة عبور على جهازك لا يمكن لأي أحد غيرك من تشغيل أواستخدام الجهاز إلا بعد ولكنها 9895 كتابتها. وهنالك كلمة عبورفي نظام التشغيل ويندوز غير مجدية وتحتاج لكثير من الجهد حتى يمكن برمجتها وجعلها مفيدة. وهناك أيضا كلمة عبور يمكن وضعها إذا كنت متصلا بشبكة معينة حيث لا يتم الاتصال إلا بعد إدخالها.

عليك بنسخة أصلية وحديثة من برنامج مضاد للفيروسات. وذلك لأنك سوف تتمتع بخدمة مجانية وغالبا ما تكون لمدة عام وهي خدمة التحديث المباشر من موقع الشركة المنتجة وهذا غير متوفر للنسخ المقلدة.
واحرص على تجديد وتحديث نسختك كل اسبوع أوعشرة ايام وذلك لظهور فيروسات جديدة أونسخ معدلة من فيروسات قديمة كل يوم.
تجنب تنزيل أوتحميل أي برامج أوملفات ذات طبيعة تنفيذية خاصة من مصادرغير موثوق بها. تجنب فتح الملفات المرفقة في الرسائل الإلكترونية من مصادر غير معروفة لديك وخاصة إذا كانت من الأنواع التالية .exe.com and.bat.scr
تجنب تنزيل أي برامج مجانية (إذا لم تكن من مواقع معروفة وذات سمعة بالحفاظ على الخصوصية وكذلك تنزيل البرامج من مصادر المجموعات الإخبارية News Group أوما يعرف ب لأن الكثير من الهاكرز يتخفون تحت مظلة هذه البرامج للوصول الى جهازك.
إذا كنت تملك معلومات في غاية الأهمية أوخاصة جدا. قم باستخدام أي برنامج لتشفير معلوماتك ورسائلك الإلكترونية.
لا تقم بأي عملية شراء من شبكة الإنترنت دون التأكد من استخدام سيرفر آمن ووجود علامة القفل المغلق في المتصفح وكذلك تغير إضافي. ما يعني (s) وهنا نلاحظ وجود حرف https://. إلى http:// أنك تستخدم بروتوكولاً آمناً لنقل المعلومات ولكن عليك التأكد أنك تستخدم قوة تشفير 128 بت وذلك لتوفير الأمان اللازم ويمكنك التأكد من قوة التشفير في متصفحك (انترنت إكسبلورر) وذلك بالنقرعلى Help وهوموجود على الجانب الأيسر من شاشة المتصفح في أعلى الصفحة ومن ثم اختيار About Internet Explorer وسوف تجد كلمة Cipher 128 bit. فإن لم تجد هذا الرقم قم بتنزيل نسخة جديدة من موقع ويندوز.
تجنب الموافقة على حفظ اسم المستخدم وكلمات العبور في أي وقت. لأنك لو وافقت على ذلك فسوف تسهل العملية على الهاكرز لأنه سوف يجدها مخزنة وجاهزة له. وينبغي عليك ألا تسمح لأي كان خاصة من موقع شخصي أوغير متخصص بإجراء تجربة على جهازك ومسح المنافذ المفتوحة فهناك العديد من الهاكرز يتخفون تحت هذا القناع ويخدعونك بهذه الحيلة لتنزيل برامج التجسس والتعرف على نقاط الضعف في جهازك أو شبكتك.

مصادر التهديد الأمني في الرسائل الإلكترونية

أولا: الملفات المرفقة التي تتطلب الفتح والتحميل: عليك بالحذر الشديد عند فتح الملفات الملحقة بالرسائل الإلكترونية لأنها أكثر الطرق استخداما من قبل أشرار الإنترنت. ولذلك ننصحك بعدم فتح الملفات المرفقة اذا كانت من أحد الأنواع التالية. وخاصة إذا لم تكن من شخص معروف لديك. وهذه الملفات الملحقة الخطيرة تنتهي بأحد هذه الاختصارات:

((COM)=(Command Files. وهذا يعني وجود ملف به أوامر للتنفيذ مرتبطة بأي جزء من الملف. وتبدأ بالعمل بعد مرور وقت معين أوحين الضغط على جزء معين.

((BAT)= (Batch Files. وهذا يعني وجود أمر معين موجه لأحد ملفات نظام التشغيل في جهازك.

((APP)= (Application وهذا يعني وجود ملف به برنامج تطبيقي وهي خطيرة لأنها ممكن أن تكون أحدبرامج التجسس.

ثانيا: الملفات المرفقة ذاتية التشغيل:

وهي قادرة على أن تقوم بالعمل حال فتحك لبرنامج البريد الإلكتروني ودون الحاجة لفتح المرفقات وتقوم بإعادة تحميل نظام التشغيل لديك ومن ثم العمل في الخفاء. وتقوم بإضافة نفسها في كل رسالة ترسلها دون علمك لتصيب بها بقية المستخدمين ومن أهم الأمثلة على ذلك. والطريقة الوحيدة لحماية نفسك من مثل هذه النوع هوإلغاء وحجب خاصية WScript.kak :ملف من متصفحك Alow Scripting.

ثالثا: بقة نظام التشغيل دوس:

هذا مصدر تهديد يسمح لمرسل الرسالة أوالصفحة من تخريب وتعطيل جهازك حال فتحك لرسالته. التي يتم فيها استخدام لغة الترميز اتش تي إم إل. لأنه من الممكن زرع تعليمات وبرامج مستخدمة في نظام التشغيل القديم وهو مايعرف بنظام دوس. ليتم تعطيل نظام ويندوز. وأكثر نظم التشغيل التي يمكن أن تتأثر بها هي نظام التشغيل ويندوز 95 و98 لأنهما يعتمدان على دوس 16 بت. وفي هذا النظام القديم توجد بعض الأوامر التي تمكن نظام التشغيل من التعامل مع بقية المكونات. ومنها على سبيل المثال للتعامل مع الطابعة والمودم وهي LPT1 for:وتكمن المشكلة في تعرف نظام printerCOM1. COM2 for communication and Fax modem. التشغيل ويندوز على هذه الأوامر القديمة والتي لا تستخدم في ويندوز حاليا ولكنها في نفس الوقت تتعرف على البرامج والأوامر القديمة إذا ما تم زرعها في لغة الترميز وهي تسبب بعض المشاكل لأنها تجعل نظام ويندوز يتبادل المعلومات والأوامر مع المكونات مثل الفاكس مودم والطابعة بدلا من القرص الصلب وبالتالي يتوقف الجهاز عن العمل ولذلك ينصح كل من يستخدم ويندوز 98 او95 بالقيام بتحديث الملفات من موقع الشركة لتغطية هذا العيب.

أشهر الفيروسات

من أشهر الفيروسات التي تنتشر عن طريق الرسائل الإلكترونية:

I Love You

Meet Melissa

Buble Boy

Yaha

Nimda

Kletz

مصادر تهديد الخصوصية والإزعاج

أولا: المتطفلون والمتجسسون على بريدك الإلكتروني:

كثير من الناس مصابون بإدمان التجسس على الغير. وينشأ معهم حب التجسس وهي كثيرة ومتنوعة ومتوفرة بالأسواق أوعن طريق الإنترنت. ويتمكنون من تحقيق ذلك بعدة طرق منها: التتبع لخصوصيات الناس برامج تخمين كلمات العبور السهلة التي قد يستخدمها الأصدقاء كاسم الدولة أوالمدينة التي ولدت بها أواسم المدرسة أوتاريخ الميلاد.

استخدام برامج مخصصة للوصول الى كلمات العبور وهي عبارة عن برامج تمكن مستخدمها من تجريب عدة آلاف من الكلمات السرية المنطقية والشائعة لدى الناس. وبذلك يمكن لها أن تصيب في بعض الأحيان.

كما يمكن لكل من يستطيع الوصول الى جهازك في المكتب أوالمنزل من الزملاء أوالأهل أوالأصدقاء من التطفل على رسائلك باستخدام بعض الخصائص المتوفرة في متصفحك ومنها: خاصية الرجوع للخلف في المتصفح. واستخدام خاصية تذكر اسم المستخدم وكلمة العبور. واستخدام خاصية الإكمال التلقائي للاسم وفراغات النماذج. واستخدام خاصية تذكر الصفحات التي تقوم بزيارتها.

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 أولغرض بيعها لإحدى الشركات. وقد انتشرت مؤخرا رسائل باللغة العربية تحكي قصص محزنة لأطفال أوكبار تعرضوا لحوادث شخصية أوحوادث 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 إنت 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 فيروس أوبرنامج تجسس أو برنامج للتحكم وتعطيل المواقع وأنت لاتعلم عنها. كما انتشرت في الآونة الاخيرة 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 التشويق للشامبو الخاص بهم.

سبل الوقاية

وللوقاية والحماية أثناء استخدام البريد الإلكتروني يجب اتباع الآتي:

*استخدام برامج مضادة للفيروسات وبرامج حماية وبرامج التشفير المتخصص.

*استخدام كلمات عبور سهلة التذكر ولكن صعبة التخمين كأن تكون مكونة من حروف وأرقام أوخليط 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 اذا كانت من أحد الأنواع التي تم ذكرها في البداية.

*عدم تحويل الرسائل المشبوهة الى أصدقائك ومعارفك.

تعديل خاصية الأمن في المتصفح الى المستوى المتوسط أوالأعلى مع تعطيل خاصية الجافا سكريبت. *في خاصية الأكتف إكس وتعديل مستوى الأمن.

عند الإنتهاء من قراءة الرسائل عليك بالخروج بطريقة صحيحة من الموقع لأن هنالك بعض أوالبرنامج ويكون ذلك بتسجيل الخروج أومايعرف ب Sign out. برامج البريد أوالمواقع تتذكرك لمدة تصل الى 8 ساعات وترحب بك مباشرة حال دخول أي شخص آخر للموقع ذاته.

وهكذا. وباطلاعك على هذه المسائل الأمنية وإدراكك الخطر الذي يهدد أمن المعلومات الخاصة بك. ستكون قادرا مستقبلا على التعامل الآمن مع ثغرات الخطر الكامنة عند استخدامك شبكة الإنترنت بشكل عام بكل ما تحتويه من تطبيقات مفيدة دخلت في صميم أسلوب الحياة الذي تعيش وخاصة في الفترة الأخيرة.

عمل الطالبة: فرجة عبدالهادي

الصف: 11