هل تعتقد أنك آمن أمام حاسوبك؟ فكّر ثانية!

كتبه فريق التحرير | 11 مارس ,2016

أصبح الإنترنت جزءا من حياتنا، فمنه نستقي المعلومة ونتعرف على العالم ونكتشف أشياء جديدة كل يوم، ولكن هل نحن آمنون أمام أجهزتنا؟ ماذا لو كان هناك من يراقبنا أو يتجسس علينا؟ ماذا لم تمكن أحدهم من سرقة معلوماتنا؟ وماذا لو تمكن أحدهم من تعقبنا ومعرفة كل شيء عنا وعن حياتنا بأدق تفاصيلها؟ وهل هذا ممكن؟

هناك العديد من الأشياء التي يجب أن ننتبه لها عند استخدام الإنترنت، فرغم أن الشبكة العنكبوتية هي مصدر لا ينضب للمعلومة، كما أنها قربت المسافات وحولت العالم إلى قرية صغيرة كما يقال، إلا أنها أيضا جعلتنا عرضة للكثير من المخاطر التي قد لا ننتبه لها أو نعي وجودها، فهناك مخترقون يمكنهم ببساطة اختراق جهازك وسرقة معلوماتك وصورك واستغلالها في أشياء يمكن أن تسيء إليك وقد تدمر حياتك.

قد يقول البعض أن هذا نوع من المبالغة ولكنها الحقيقة التي تثبتها العديد من التجارب التي ربما تكون أنت أيضا قمت بالقراءة عنها أو مشاهدتها في نشرات الأخبار، لأن نهايتها كثيرا ما تكون مفجعة.

الهدف ليس تخويفك ولكن الهدف هو توعية المستخدم إلى أن هناك أخطار تتربص به كلما فتح جهازه وجلس أمامه، ولذلك فقد أصبحنا نسمع عما يسمى " الأمن المعلوماتي".

وحتى تتجنب كلما ذكر سلفا هناك أشياء عليك أولا أن تفهمها وهناك خطوات يجب أن تلتزم بها، والغريب أن النصائح التي ستتعرف عليها معنا في هذا المقال هي من مخترقين أو ما يسمى بالهاكرز، وهذا ليس غريبا حيث أن المخترق عادة ما يكون ملما بشتى أنواع الحماية وسبلها:

حافظ على أمن معلوماتك:

وهذا يعني إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، وعدم إمكانية الوصول إليها من قبل أي شخص آخر دون إذن منك، ووعليك أن تكون ملما بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصة، فمن الواضح أن معظم الأشخاص يرغبون في الحفاظ على خصوصية معلوماتهم الحساسة مثل كلمات المرور ومعلومات البطاقة الائتمانية وعدم تمكن الآخرين من الوصول إليها، والكثير من الأشخاص لا يدركون بأن بعض المعلومات التي قد تبدو تافهة أو لا معنى لها بالنسبة لهم فإنها قد تعني الكثير لأناس آخرين وخصوصاً إذا ما تم تجميعها مع أجزاء أخرى من المعلومات، فعلى سبيل المثال، يمكن للشركة الراغبة في الحصول على معلومات شخصية عنك للأغراض التسويقية أن تشتري هذه المعلومات من شخص يقوم بتجميعها من خلال الوصول إلى جهاز كمبيوترك بشكل غير شرعي، ومن المهم كذلك أن تفهم أنك حتى ولو لم تقم بإعطاء معلوماتك لأي شخص عبر الإنترنت، فقد يتمكن بعض الأشخاص من الوصول إلى نظام الكمبيوتر لديك للحصول على المعلومات التي يحتاجونها دون علم أو إذن منك.

تجنب الهاكرز و المخترقين و الفيروسات واللصوصية:

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي، وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة، وهؤلاء الأشخاص عادة ما يستخدمون برامج ضارة يزرعونها في مواقع أو تطبيقات أو برامج وهي التي تمكنهم من الولوج إلى أجهزة ضحاياهم، ولتجنب الوقوع في براثنهم لابد من حماية جهازك من خلال تثبيت برامج الحماية، وبرامج الجدار الناري، وعدم تجاهل تحذيرات برامج الحماية المثبتة على الجهاز مهما كانت الإغراءات.

فيروسات الكمبيوتر هي الأكثر شيوعاً من بين مشاكل أمن المعلومات التي يتعرض لها الأشخاص والشركات، وفيروس الكمبيوتر هو برنامج غير مرغوب فيه يدخل إلى الجهاز دون إذن ويقوم بإدخال نسخ من نفسه في برامج الكمبيوتر، وهو أحد البرامج الخبيثة أو المتطفلة، أما البرامج المتطفلة الأخرى فهي تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس.

يمكن للبرامج الخبيثة أن تسبب الإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطيئه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها، أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك، أما بالنسبة لبرامج الدعاية وبرامج التجسس فهي مزعجة في الغالب وتؤدي إلى ظهور نوافذ دعائية منبثقة على الشاشة،كما أن برامج التجسس تجمع معلوماتك الشخصية وتقدمها إلى جهات أخرى تطلب الحصول عليها لأغراض تجارية.

أما اللصوصية أو (Phishing) فهو عمل إجرامي يتمثل في سرقة الهوية، حيث يقوم شخص أو

شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة نظامية ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول الى الموقع، وهناك برامج لمكافحة هذا النوع من التطفل واكتشاف هوية المرسل الحقيقي، ولكن أفضل وسيلة للحماية هي الحذر و الوعي فليس هناك بنك أو مؤسسة مالية تطلب من عملائها إرسال معلوماتهم الشخصية من خلال البريد.

إذن هل هناك بالفعل خصوصية على الإنترنت؟

الجواب هو لا بصراحة وبكل بساطة فأنت مراقب طيلة فترة تواجدك أمام جهازك، فمحركات البحث تستخدم ما يسمى بالكوكيز للتعرف على اهتماماتك وتظهر لك ما يهمك وما تبحث عنه بكثرة، وهذا ليس سرا، أما بريدك الإلكتروني فإن خصوصيته أشبه بخصوصية البطاقة البريدية، فقبل أن تسلم رسائلك تمر هذه الأخيرة عبر العديد من الخوادم حيث يمكن الوصول إليها من قبل الأشخاص الذين يديرون النظام وأيضا الأشخاص الذين يتسللون إليه بشكل غير نظامي، والطريقة الوحيدة للتأكد إلى حد ما من خصوصية بريدك الإلكتروني هو تشفيره.

ماذا تفعل لتحمي نفسك؟

هناك خطوات يمكنك القيام بها لحماية نفسك وهي في الواقع نصائح من أحد المخترقين الفرنسيين التائبين ويدعى Hugo، والذي ينصح المستخدمين:

1- اختيار كلمات مرور معقدة وتغييرها بشكل منتظم، حيث أن الغالبية العظمى من الناس

تستخدم نفس كلمة السر لجميع حسابات البريد الإلكتروني الخاصة بهم وهذا خطأ فادحا، وينصح هوغو باختيار كلمة مرور معقدة مكونة منالحروف والأرقام الكبيرة والصغيرة.

2- اختيار جدار حماية وبرنامج مكافحة الفيروسات جيد، علما أنه لا يوجد نظام منيع لا يمكن اختراقه لكن هذه البرامج يمكن أن تجعل مهمة المخترق أطول وأصعب.

3- تثبيت مفتاح WPA 2 على شبكتك الاسلكية، حيث أن هناك أنواع عديدة من المفاتيح اللاسلكية، ويعتبر مفتاح WEP الأكثر شيوعا، لأنه لا يزال عادة الخيار الافتراضي في معظم المعدات، ولكنه أيضا أقل أمنا، ويمكن فك تشفير مفتاح WEP في 3 إلى 5 دقائق" بينما يتطلب فك شفرة WPA 2 من 11إلى 16 ساعة .

4- الحرص على فصل الواي فاي في المساء، في الليل، وعند الانتهاء من استخدام جهاز الكمبيوتر، قم بإيقاف الواي فاي، ذلك أن بقائه مشغلا يجعله يبسهل على المخترقين التسلل إلى جهازك من خلال الشبكة التي تشكل جسرا، وبالتالي فإن فصله يجعل شبكتك في أمان.

5- الحرص على وضع قطعة صغيرة من الورق على كاميرا الويب، فذلك يجعلك بعيدا عن أعين المتطفلين الذين يمكن أن تسول لهم أنفسهم مراقبتك.

أخيرا يقول هوغو أن برنامج حصان طروادة كان يسهل عليه مراقبة ضحاياه، وفي العام الماضي كشف تحقيق لبي بي سي وجود مواقع متخصصة حيث يتبادل القراصنة الصور المسروقة، ويذهب بعض المتسللين إلى أبعد من ذلك من خلال بيع رموز الوصول لرخص الكاميرات لاختلاس النظر.

والآن بعد أن قرأت هذا الموضوع هل ستجلس أمام جهازك تماما كما فعلت بالأمس أم أنك ستتخذ بعض الإجراءات؟

رابط المقال : https://www.noonpost.com/10705/