

لماذا يعد أمن الانترنت الالكتروني مشكلة؟

من المؤكد أنك سمعت قصصاً حول سرقة أرقام بطاقات الائتمان وعن انتشار فيروسات البريد الالكتروني. وربما كنت أنت نفسك يوماً ما ضحية لمثل هذه الحوادث. إن أفضل طرق الدفاع هي فهم المخاطر. فماذا تعني بعض تلك المصطلحات الأساسية، وما الذي يجب أن تفعله لحماية نفسك؟

ما هو أمن الانترنت الالكتروني؟

إن كل شيء حولنا الآن يعتمد على الحاسوب وشبكة الانترنت والاتصالات (البريد الالكتروني والهواتف الخليوية) ، وسائل الترفيه (الكابلات التلفزيونية الرقمية ومشغلات صيغ MP3) ، وسائل النقل (الانظمة الخاصة بمحرك السيارات ، وأجهزة الملاحة الخاصة بالطائرات) ، التسوق (المخازن الالكترونية والبطاقات الائتمانية) ، المجال الطبي (الأجهزة والسجلات الطبية) .. الخ. كم تعتمد حياتك اليومية على هذه الاجهزة ومنها (الحاسوب)؟ وكم من معلوماتك الشخصية مخزنة على حاسوبك الشخصي أو على حاسوب آخر؟

يتضمن أمن الانترنت الالكتروني حماية تلك المعلومات عن طريق الحماية والكشف والاستعداد لصد الهجمات الالكترونية.

ما هي المخاطر؟

هناك العديد من المخاطر بعضها أكثر خطورة من غيرها. بين تلك المخاطر مثل فيروسات تمحو نظامك بالكامل أو شخص ما يخترق نظامك ويغير بيانات الملفات أو شخص ما يستخدم حاسوبك لمهاجمة الآخرين ، أو يقوم بسرقة معلومات بطاقتك الائتمانية ويقوم بعمليات شراء غير مجازة. لسوء الحظ فإنه لا يوجد ضمان (حماية) بنسبة 100% لجهازك حتى مع استخدام أفضل الإجراءات الوقائية ، ولكن هناك خطوات يمكنك اتخاذها للتقليل من الخطر.

ما الذي يمكنك عمله؟

الخطوة الأولى لحماية نفسك هي إدراك تلك المخاطر والاطلاع على بعض المصطلحات

المرتبطة بها.

المقتحمون ، المهاجمون ، المتطفلون - تُستخدم هذه المصطلحات لأشخاص يسعون لاستغلال الضعف في البرامج ونظم الحاسوب لأهدافهم الشخصية. ورغم أن نواياهم قد تكون أحياناً طيبة وقد يكونوا مدفوعين بالفضول فقط، فإن أعمالهم تشكل مخالفة للاستخدام المقصود للأجهزة التي يستغلونها. وقد تتراوح النتائج بين مجرد الخداع (تكوين فيروس بدون أثر سلبي مقصود) وإيقاع الضرر (سرقة أو تغيير المعلومات).

الشفرة الخبيثة "**Malicious Code**" - تشمل هذه الفئة الفيروسات والديدان وأحصنة طروادة. ورغم أن بعض الناس يستخدمون هذه المصطلحات بشكل تبادلي فإن لكل منها خصائص تجعلها منفردة عن غيرها.

- **الجرثومة - "Virus"** - الفيروسات: هذا النمط من الشفرة المضرة يتطلب منك أن تقوم بشيء ما قبل أن تهاجم حاسوب، كنتيجة لفتح بريد الكتروني يتضمن ملف مرفق، أو الدخول إلى موقع الكتروني مُعين .
- **الدودة "Worm"** - ينتشر هذا النوع دون تدخل المستخدم. حيث إنها تبدأ عادة باستخدام نقاط الضعف في البرامج (قصور يسمح بانتهاك سياسة الأمن المقصودة للبرامج) ومتى أصيب الحاسوب الضحية فإن الدودة ستحاول أن تعثر على حاسوب آخر وتصيبه. شأنها شأن الفيروس ، يمكن للدودة أن تنتشر عبر البريد الالكتروني ، مواقع الانترنت أو المواقع التي تقدم البرامج الالكترونية. إلا أن الانتشار الذاتي الآلي للديدان يميزها عن الفيروسات.
- **أحصنة طروادة "Trojan Horse"** - برنامج حصان طروادة برنامج يدعي أنه يقوم بعمل ما بينما هو في الحقيقة يقوم بشيء ما مختلف وراء الستار. على سبيل المثال فإن برنامجا ما يدعي أنه يمكن أن يجعل كومبيوترك أسرع ربما يقوم ببيث معلومات سرية لمتطفل ما عن بعد.

هذه السلسلة من المعلومات الأمنية ستجعلك أكثر معرفة بكيفية التعرف على تلك الهجمات وحماية

نفسك منها.

تأليف: مندي مكدول، وآلن هاوس هولدر
