التكنولوجيا الشطارة كبار السن

مقدمة إلى الأمان السيبراني: كيف تحافظ على أمانك على الإنترنت

أصبحت شبكة الإنترنت جزءًا لا غنى عنه في حياتنا ويمكننا القيام بالعديد من الأشياء عبر الإنترنت.

نود أن نخبرك بكيفية استخدام الإنترنت بشكل أكثر أمانًا والاحتياطات العامة لحماية خصوصيتك.

1. هل أحتاج لحماية نفسي على الإنترنت؟

على الإنترنت ، يمكن لأي شخص تزوير هويته ، لذلك عليك أن تعرف من الذي يجب عليك قبول رسائل البريد الإلكتروني منه ، ومكان التسوق الآمن ، والجهة التي يجب أن تعطي التفاصيل الخاصة بك.
يلعب برنامج أمان الإنترنت دورًا مهمًا في الحفاظ على سلامتك من الجريمة السيبرانية.
ستجعلك بضع خطوات منطقية من الصعب خداعك:
- هل لديك أجهزة الكمبيوتر والشبكات اللاسلكية محمية بكلمة مرور؟
- لا تعطِ أبدًا تفاصيل خاصة للمضاربين عبر الإنترنت.
- قم بتثبيت برنامج أمان.

2. التهديدات التي قد تواجهها

1) البرامج الضارة

البرامج الضارة (البرامج الضارة): يتم إنشاؤها بنية الوصول إلى جهاز الكمبيوتر الخاص بك وجمع المعلومات ، عادة لغرض بيعها إلى الأطراف المعنية الأخرى. النوع الأكثر شيوعًا من البرامج الضارة هو فيروس.
يجب أن تكون حذراً بشأن البرامج التي تقوم بتنزيلها وتشغيلها على جهاز الكمبيوتر الخاص بك. إذا قمت بتنزيل برنامج من مصدر سيئ السمعة ، فقد يكون مصابًا.

حتى إذا كنت تتصفح بشكل آمن ، فلا يمكنك منع الشفرة الضارة من أن تكون مصابة بنسبة 100٪ بأحدث شفرة خبيثة أو إهمال المستخدم. لذلك ، يجب تثبيت برنامج مكافحة الفيروسات على جهاز الكمبيوتر الخاص بك وتمكين الحماية في الوقت الحقيقي.
يمكن أن يكون اللقاح ضروريًا لأمن الكمبيوتر الشخصي لأنه ينفذ عمليات الفحص عندما لا يتم اكتشاف الإنترنت فحسب ، بل أيضًا الأجهزة الخارجية مثل USB و CD.

2) قراصنة

يحاول Hacker (أو bot): استغلال ثغرة أمنية في جهاز الكمبيوتر الخاص بك للوصول إلى ملفاتك الشخصية.

كمثال ، هل تعرف عن مشاركة ملفات Windows؟ يسمح ذلك لجهاز كمبيوتر واحد بإرسال المستندات إلى كمبيوتر آخر عبر شبكة. ولكن إذا لم تكن كلمة المرور

المتسللين ، وأكثر من ذلك بكثير. تحمل مجموعات أمان الإنترنت رسومًا سنوية (تتراوح عادة بين 60 و 130 دولارًا).

حماية جهاز الكمبيوتر الخاص بك
1) يعمل جدار الحماية مثل نقطة تفتيش أمنية لحركة مرور الإنترنت - لا يسمح إلا بالمرور المصرح به من خلاله.
2) يتتبع برنامج مكافحة الفيروسات أي برامج ضارة - بما في ذلك الفيروسات وبرامج التجسس والبرامج الإعلانية - ويزيلها - والتي تأتي على جهاز الكمبيوتر الخاص بك. من المحتمل أن الكمبيوتر الخاص بك لا يأتي مع برنامج مكافحة الفيروسات ، ويجب عليك تثبيته.

4. اختيار برنامج الأمان

يوصى بأن يكون أي جهاز توصله بالإنترنت - جهاز الكمبيوتر أو الجهاز اللوحي أو الهاتف الذكي - محميًا ببرامج مكافحة الفيروسات أو ، بشكل مثالي ، مجموعة أمان على الإنترنت. إذا كنت غير قادر على تحمل الرسوم السنوية ، يمكنك الحصول على تطبيق مضاد فيروسات مجاني بدلاً من ذلك. لن تحمي نظامك بالإضافة إلى مجموعة الأمان ، ولكنها ستقدم لك خطًا أساسيًا للحماية.
برامج مكافحة الفيروسات المجانية هي كما يلي:
مايكروسوفت: www.microsoft.com/securityessentials
AVG: www.avgfree.com.au
أفاست !: www.avast.com
كومودو: www.antivirus.comodo.com

5. حافظ على سلامتك (برامج الأمان ليست كافية)

يعد تثبيت برامج الأمان على جهاز الكمبيوتر الخاص بك خطوة كبيرة ومهمة في حماية نفسك عبر الإنترنت. لكن هذا ليس الحل بالكامل: لا يمكن أن تحميك برامج الأمان من المحتالين والمجرمين الإلكترونيين. تتضمن العديد من الأشياء التي نقوم بها على الإنترنت معلومات مهمة أو شخصية أو خاصة. معلوماتك الشخصية هي المعلومات التي تحدد هويتك. لحماية معلوماتك الشخصية ، يجب توخي الحذر بشأن ما تشاركه بشكل عام عبر الإنترنت.

سوف الحس السليم وجرة صحية من الشك تجعلك من الصعب جدا احتيال!

هناك بعض الأشياء البسيطة التي يمكنك القيام بها للحفاظ على أمانك:

1) استخدم كلمة مرور / كلمة مرور قوية وفريدة من نوعها ، وقم بتغييرها بشكل منتظم
2) لا تنشر معلومات شخصية على المواقع العامة
3) لا تفتح مرفقات البريد الإلكتروني ما لم تكن متأكدًا حقًا
4) توخ الحذر بشأن الرسائل الإلكترونية التي ترد عليها
5) كن حذرا من إعطاء تفاصيل بطاقة الائتمان ل
6) لا تثبت برامج من مصادر غير موثوقة

محميًا ، قد يكتشف المخترق ذلك ويستخدمه للوصول إلى ملفاتك أو زرع فيروس أو أي نوع آخر من البرامج الضارة على جهاز الكمبيوتر.

3) سرقة الهوية ، والتصيد الاحتيالي والمحتالين

لا توجد قواعد حول من يمكنك القول بأنك على الإنترنت ، بحيث يمكن للناس محاولة التظاهر بأنهم شيء أو شخص ما ليس من أجل الحصول على أموال أو كشف معلومات شخصية مثل أرقام بطاقات الائتمان وعبر الإنترنت عمليات الدخول المصرفية. في الأساس ، أخذ المشاغبون نشاطهم التجاري عبر الإنترنت ، وهم يحاولون الاستفادة منك. الخداع الشائع هو محاولة التصيّد الاحتيالي ، حيث يتظاهر المخادع بأنه شخص أو مؤسسة تربطك علاقة بها ، ويمنحك القدرة على التخلي عن المعلومات الخاصة ، مثل تفاصيل حسابك المصرفي.

هناك بعض الطرق البسيطة للمساعدة في التعرف على الرسائل غير المرغوب فيها والتصيد الاحتيالي وتجنب الوقوع في المشاكل على الإنترنت. إليك بعض الأشياء التي يجب الانتباه إليها.

• تحقق من موضوع البريد الإلكتروني والمرسل. هل هي من شخص تعرفه ، وهل تصف شيئًا تتذكر أنه اشترك فيه؟ إذا لم يكن كذلك ، فمن المحتمل أن يكون غير مرغوب فيه.
هل هناك عرض مالي مجاني مقابل معلوماتك الشخصية؟ هل تعد بالعواقب السلبية إذا لم ترد على المعلومات الشخصية ، أو بالنقر أو الرابط؟ هل لها اسمك في الحقل؟ هذه كلها علامات على احتيال التصيد.
• هل يحتوي البريد الإلكتروني على أخطاء إملائية ونحوية ، وهل يتم تقديمها بشكل سيئ؟ هل البريد الإلكتروني من حساب بريد إلكتروني مجاني (outlook.com، yahoo.com، gmail.com)؟ إذا كان الأمر كذلك ، وكان المرسل غير معروف لك ، تعامل معه بشك.

يمكن أن تكون رسائل البريد الإلكتروني "Vanity scam" جذابة للغاية ، ويبدو الكثير منها أصليًا. إذا كنت تجرّب ، فتأكد من سؤالك عن سبب تلقيك مثل هذه الرسالة الإلكترونية ، مثل الأسماء والعناوين والمواقع الإلكترونية.

3. ماذا تفعل برامج الأمان؟

أنواع البرامج الأمنية
والخبر السار هو أنه يمكنك حماية نفسك من معظم الهجمات باستخدام برامج الأمان. يأتي الكمبيوتر الخاص بك مع بعض برامج الأمان المضمنة ، ولكن يجب إضافة برامج إضافية فوق ذلك. هناك أنواع مختلفة من برامج الأمان التي يمكنك الحصول عليها:

1) Antivirus: برنامج يحمي جهاز الكمبيوتر الخاص بك من معظم أنواع البرامج الضارة (ويعتمد على دفاعات الكمبيوتر المضمنة الخاصة بالباقي). يمكنك الحصول على برنامج مكافحة الفيروسات مجانًا أو مقابل رسوم بسيطة.
2) مجموعات أمان الإنترنت: مجموعة من البرامج التي تحمي جهاز الكمبيوتر الخاص بك من مجموعة كاملة من التهديدات ، بما في ذلك البرامج الضارة والمخادعين والبريد الإلكتروني غير الهام ومواقع ويب الخادعة