

التكنولوجيا الشطاره كبار السن

مقدمة إلى الأمان السيبراني: كيف تحافظ على أمانك على الإنترنط



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 الفاح ضروريًا لأمن الكمبيوتر الشخصي لأنه ينفذ عمليات الفحص عندما لا يتم اكتشاف الإنترنط فحسب ، بل أيضًا الأجهزة الخارجية مثل CD و USB.

2. قراصنة

يحاول Hacker استغلال ثغرة أمنية في جهاز الكمبيوتر الخاص بك للوصول إلى ملفاتك الشخصية.

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

حماية جهاز الكمبيوتر الخاص بك

(1) يعمل جدار الحماية مثل نقطة تفتيش أمنية لحركة مرور الإنترنط - لا يسمح إلا بالمرور المصرح به من خالله.

(2) يتبع 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.

أصبحت شبكة الإنترنط جزءاً لا غنى عنه في حياتنا ويمكننا القيام بالعديد من الأشياء عبر الإنترنط نود أن نخبرك بكيفية استخدام الإنترنط بشكل أكثر أماناً والاحتياطات العامة لحماية خصوصيتك..

1. هل أحتاج لحماية نفسى على الإنترنط؟

على الإنترنط ، يمكن لأى شخص تزوير هويته ، لذلك عليك أن تعرف من الذى يجب عليك قبول رسائل البريد الإلكتروني منه ، ومكان التسوق الآمن ، والجهة التي يجب أن تعطى التفاصيل الخاصة بك.

يلعب برنامج أمان الإنترنط دوراً مهماً في الحفاظ على سلامتك من الجريمة السيبرانية.

بعض خطوات منطقية ستجعلك من الصعب خداعك :

- هل لديك أجهزة الكمبيوتر والشبكات اللاسلكية محمية بكلمة المرور الخاصة بك؟
- قم بتنصيب برنامج أمان.

2. التهديدات التي قد تواجهها

1. البرامج الضارة

البرامج الضارة: يتم إنشاؤها بنية الوصول إلى جهاز الكمبيوتر الخاص بك وجمع المعلومات ، عادة لغرض بيعها إلى الأطراف المعنية الأخرى. النوع الأكثر شيوعاً من البرامج الضارة هو فيروس.

- لا تعطِ أبداً تفاصيل خاصة للمضارعين عبر الإنترنط.
- يجب أن تكون حذراً بشأن البرامج التي تقوم بتزييلها وتشغيلها على جهاز الكمبيوتر الخاص بك. إذا قمت بتنزيل برنامج من مصدر سيئ السمعة ، فقد يكون مصاباً.

3. سرقة الهوية ، والتصيد الاحتيالي والمحاتلين

ليس هناك أي قواعد لإظهار حقائق أهداف الناس 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 وغير الإنترنت عمليات الدخول المصرفية. في الأساس ، أحد المشاغلون نشاطهم التجاري عبر الإنترنت ، وهم يحاولون الاستفادة منه. الخداع الشائع هو محاولة التصيد الاحتيالي ، حيث ينطaher المخادع بأنه شخص أو مؤسسة تربطك علاقه بها ، وينمّح القرة على التخلّي عن المعلومات الخاصة ، مثل تفاصيل حسابك المصرفى.

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 شيئاً تذكر أنه اشتراك 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 الحق؟ هذه كلها علامات على احتيال التصيد.

• هل يحتوي البريد الإلكتروني على أخطاء إملائية ونحوية ، وهل يتم تقديمها بشكل سيء؟ هل البريد الإلكتروني من حساب بريد إلكتروني مجاني (gmail.com، yahoo.com، outlook.com)؟ إذا كان الأمر كذلك ، وكان المرسل غير معروف لك ، تعامل معه بشك.

يمكن أن تكون رسائل البريد الإلكتروني "Vanity scam" جاذبة للغاية ، ويبدو الكثير منها أصلياً. إذا كنت تجرّب ، يجب ان تسأل نفسك عن سبب ثقتك مثل هذه الرسالة الإلكترونية ، مثل الأسماء والعناوين والموقع الإلكترونية.

4. مادا 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 مجاناً 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 والمخدعين والبريد الإلكتروني غير الهام ومواقع ويب الخادعة

5. اختيار برنامج الأمان

يوصى بأن يكون أي جهاز متصله بالإنترنت - جهاز الكمبيوتر أو الجهاز اللوحي أو الهاتف الذكي - محمياً 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 خطأ أساسياً للحماية.

برامج مكافحة الفيروسات المجانية هي كما يلي:

www.microsoft.com/securityessentials: مایکروسوفت

AVG: www.avgfree.com.au

www.avast.com

www.antivirus.comodo.com

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 وال مجرمين الإلكترونيين. تتضمن العديد من الأشياء التي تقوم 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.

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

- ١) استخدم كلمة مرور / كلمة مرور قوية وفريدة من نوعها ، وقم بتبديلها بشكل منتظم
 - ٢) لا تنشر معلومات شخصية على المواقع العامة
 - ٣) لا تفتح مرفقات البريد الإلكتروني ما لم تكن متأكداً حقاً
 - ٤) توخي الحذر بشأن الرسائل الإلكترونية التي ترد عليها
 - ٥) كن حذراً من إعطاء تفاصيل بطاقة الائتمان
 - ٦) لا تثبت برامج من مصادر غير موثوقة

خلاف المسؤولية المعلومات الواردة في هذا المنشور وأي مواد مراقبة لها هي فقط للأغراض التعليمية والإعلامية. لا يجوز أن يشكل المنشور وأي مواد مراقبة الترويج له أو تأييده أو تأييده لأي منتج أو خدمة مشار إليها أو موضحة في المنشور وأي مواد مراقبة. الغرض من المنشور وأية مواد مصاحبة هو استخدامه كمرجع أولي فقط. ليس الغرض منها أن تكون دليلاً شاملًا أو تطبيقي في جميع الحالات. بذلك جهود معقولة لضمان صحة المعلومات التي تظهر في هذا المنشور وأي مواد مصاحبة في وقت الإنتاج. ومع ذلك، فإن مؤلفي ومنتجي ومقدمي هذا المنشور وأي مواد مراقبة (الأشخاص ذوي الصلة) * لا يمثلون أو يضمونون دقة أو موثوقية أو اكتمال أو عملة المعلومات في هذا المنشور وأي مواد مراقبة. يتم توفير المعلومات وأية نصيحة يتم تقديمها في هذا المنشور وأي مواد مراقبة فقط على أساس أن الجمهور سيكون مسؤولاً عن إجراء تقديرهم الخاص للقضايا التي تمت مناقشتها هنا وتنصح بالتحقق من جميع البيانات والبيانات * الأشخاص ذوي الصلة. • استبعاد، إلى أقصى حد يسمح به القانون، جميع الضمانات الصريحة أو الضمنية من أي نوع فيما يتعلق والمعلومات ذات الصلة بأي معلومات في هذا المنشور وأي مواد مراقبة؛ • ليست ملزمة بتحديث أي معلومات في هذا المنشور وأي مواد مراقبة أو تصحيح أي عدم دقة في هذا المنشور وأي مواد مراقبة قد تصبح واضحة في وقت لاحق؛ تحفظ لنفسها بالحق ، حسب تقديرها المطلق ، في حذف أو تغيير أو نقل المنشور (وأي مواد مراقبة) وأي من محتوياته (بما في ذلك شروط وأحكام إخلاء المسؤولية) في أي وقت دون إشعار. * يشمل الأشخاص ذوي الصلة أي فرد أو شركة أو شراكة أو إدارة حكومية معنية بإعداد النشر والمسؤولين المعينين والموظفين وال وكلاء. إشعار تجاري قد تكون جميع أسماء المنتجات أو موقع الويب المشار إليها في هذا Google Play و Google وAndroid المنشور التعليمي علامات تجارية مسجلة أو علامات تجارية لأطراف ثالثة في أستراليا / أو بلدان أخرى. تعد مسجلة في Apple Inc. هي علامات تجارية لشركة iPad أو iTunes Store أو App Store و iTunes أو Apple Inc. علامات تجارية لشركة Google Inc. في إما علامات تجارية مسجلة أو علامات تجارية لشركة Microsoft Corporation و Windows و Microsoft و Microsoft Corporation الولايات المتحدة وبلدان أخرى ، أما الولايات المتحدة وأستراليا. لا توجد علامات تجارية لأطراف ثالثة ضمن هذه المادة تعكس ارتباطاً أو ارتباطاً أو تأييده أو رعاية لهذه المواد من قبل تلك Telstra Corporation Limited (ABN 33 051 775 556)الأطراف الثالثة. إشعار الملكية الفكرية وإخلاء المسؤولية حقوق الطبع والنشر © ساوث ويلز للشيخوخة. جميع الحقوق محفوظة. المواد محمية بموجب حقوق الطبع والنشر بموجب قوانين أستراليا ومن خلال المعاهدات الدولية وبلدان أخرى. لا يجوز إصدار أي جزء من هذه المواد أو توزيعها أو إعادة إنتاجها أو نسخها أو تخزينها أو نقلها بأي شكل أو بأي وسيلة ، سواء كانت إلكترونية أو ميكانيكية أو تسجيل أو غير ذلك ، لمعلوماتك أو أحالتك أو دراستك.