الخليج

اقتصاد, تقنية وسيارات

12 فبراير 2022 15:02 مساء

كيف تحمي بياناتك الشخصية والمالية من الاحتيال؟



دبي: عبير أبو شمالة

يؤكد الخبراء دوماً، أهمية الحفاظ على البيانات الشخصية والمالية للمرء تفادياً لسقوطه في حبائل المحتالين والتعرض للاحتيال؛ ويوصي الخبراء بخطوات قليلة لكنها على درجة كبيرة من الأهمية وقادرة على مساعدتك في التخلص من عمليات الاحتيال.

ومن أبرز الخطوات الموصى بها لحماية معلوماتك الشخصية وحماية نفسك من عمليات الاحتيال على الهوية بحسب توصيات الإمارات دبي الوطني:

تحديث برنامج التصفح الخاص بك

توفّر نسخ برنامج التصفح الأحدث الحماية ضد مواقع الإنترنت المزيفة.

يسمى البرنامج الذي تستخدمه للمشاهدة والبحث في مواقع الإنترنت برنامج التصفح. تقوم برامج التصفح الحديثة بتحذيرك عندما تتصفح المواقع المزيفة وسيكون من الصعب على الفيروسات أن تخترقها.

ومن الجيد أن تقوم بتنزيل وتثبيت برنامج تصفح محدّث، وهناك العديد منها لتختار من بينها وجميعها مجانية.

حافظ على تحديث البرامج الخاص بك

من الصعب على الفيروسات إصابة البرامج التي يتم تحديثها باستمرار.
محدث أو لا من خلال الذهاب إلى Windows يمكنك التحقق إذا كان جهاز الكمبيوتر الخاص بك يعمل بنظام ويندوز
أما بالنسبة لنظام التشغيل من نسخة .Windows 7 في نظام التشغيل "Action Center - «مركز الإجراءات
.Windows في نظام"Settings – فستجد روابط التحديث والأمان في قائمة»الإعدادات Windows 10
● يستغل المجرمون الذين يصنعون الفيروسات الأخطاء وأماكن الخلل في برمجيات البرامج كي يقوموا بالوصول إلى أجهزة الكمبيوتر الأخرى.
● لذلك تعمل شركات البرامج على إصلاح هذه الأخطاء وتوفيرها للمستخدمين من خلال تحديثات مجانية قابلة للتنزيل، لذلك سيكون من الجيد أن تقوم بتثبيت التحديثات الخاصة بالبرنامج بمجرد توفرها.
● كن حذراً من رسائل البريد الإلكتروني المزيفة التي تطلب القيام بعملية التحديث للبرامج. استخدم برنامج التحديث المصاحب للكمبيوتر الخاص بك ولا تضغط على الروابط المدرجة في هذه الرسائل.
● بالإضافة إلى برامج النظام الخاصة بالكمبيوتر، فإن عملية التحديث يجب أن تطال البرامج الأخرى الموجودة في الكومبيوتر. وهذا يشمل برنامج تصفح الإنترنت والتطبيقات التي تستخدمها. ستتحقق معظم البرامج الحديثة من التحديثات بشكل تلقائي، ويفضل هنا أن تقوم بتثبيت هذه التحديثات حالما تصبح متوفرة.
لا تشارك المعلومات الخاصة على الإنترنت
الخاصة بمواقع شبكات التواصل الاجتماعي. (Privacy Settings) تحقق مرتين من إعدادات الخصوصية
ما هو اسم أول مدرسة التي ذهبت إليها؟ ماهو عنوانك؟ عيد الميلاد؟ رقم الهاتف؟ كل هذه المعلومات مفيدة للأشخاص الذين يرغبون في سرقة هويتك أو في الوصول إلى حسابك المصرفي عبر الإنترنت. بالطبع أنت لن تعطي هذه المعلومات إلى شخص غريب تقابله في الشارع، ولكن إذا كنت تستخدم مواقع شبكات التواصل الاجتماعي، مثل فيسبوك أو تويتر، فسيكون من المحتمل أنك بالفعل تفرط في مشاركة بعض بياناتك الشخصية.
قد ترغب جدياً في التفكير بعناية في المعلومات التي تضعها في ملفاتك الشخصية على مواقع مثل هذه. سيكون من الجيد أيضاً أن تقوم بالتحقق من إعدادات الخصوصية في كل موقع تستخدمه للتأكد من أنك تشارك معلوماتك الشخصية مع الأشخاص الذين تثق بهم فقط.
اعتن وحافظ على كشوف الحساب الورقية
يحاول المحتالون الوصول إلى المعلومات الشخصية من مصادر مختلفة وذلك لسرقة هويات الأشخاص.
الفيروسات هي إحدى الطرائق التي يقومون بذلك من خلالها، ولكنهم يستخدمون أيضًا مستندات حسابك الورقية التي تحتوي على تفاصيل شخصية، مثل الإيصالات وكشوف الحساب المصرفي. ويستخدم المحتالون العديد من الطرق مثل البحث في صناديق القمامة للحصول على هذه المستندات.
يجب أن تتخذ احتياطات بسيطة للحفاظ على بياناتك آمنة وهذا سيستوجب منك التخلص من هذه المستندات بأمان، مثل تمزيقها قبل رميها في صندوق القمامة.
إليك الطرق التي يستخدم المجرمون فيها الإنترنت للوصول إلى هدفهم
هدف المجرمين من كل ما سبق هو الحصول على المال
وهناك العديد من الطرق لكسب الأموال عبر الإنترنت:
● القيام بسرقة كلمات المرور الخاصة بك والتفاصيل المصرفية من خلال الفيروسات، رسائل البريد الإلكتروني المزورة ومواقع الإنترنت المزيفة
● الاحتيال عليك كي تقوم بتزويدهم بمعلومات أمنية
تحت غطاء عروض ومنتجات وهمية (Spam) ● إرسال رسائل بريد إلكترونية مؤذية

- الوصول إلى جهاز الكمبيوتر الخاص بك واستخدامه لمهاجمة أجهزة الكمبيوتر الخاصة بالأشخاص الآخرين
- استخدم الفيروسات لعرض إعلانات غير مرغوب فيها على جهاز الكمبيوتر الخاص بك

تجنب عمليات الاحتيال والخداع عبر الإنترنت

أحياناً سيكون العرض مغرياً لدرجة أنه سيصعب تصديقه. عندما يتعلق الأمر بحماية نفسك وأموالك على الإنترنت، كن حذراً من عروض الصفقات السخيفة. قد يحاول المجرمون التواصل معك من خلال رسائل البريد الإلكتروني، أو عبر أو حتى عبر الهاتف. لذلك، من المفيد هنا أن SMS مواقع الإنترنت التي تستخدمها، أو عبر الرسائل النصية القصيرة تكون دائماً على حذر لأن هذه المحاولات قد تكون أحياناً مقنعة تماماً وقريبة للحقيقة كثيراً.

فيما يلي بعض العلامات التحذيرية:

- وعود كبيرة: «لقد ربحت اليانصيب»
- تهديدات كبيرة: «لقد تم اختراق حسابك»
- شعور زائف بضرورة الرد: «عليك اتخاذ قرارك الآن أو سوف يفوت الأوان»
- السرية غير الضرورية: «لا تخبر أحداً»
- ألا يكون هناك أي سبب واضح لهم للاتصال بك. فمثلاً: هل قمت حتى بشراء تذكرة يانصيب لتربح اليانصيب أصلاً؟
- «فرص العمل» التي تنطوي على إبقاء أو تلقي الأموال من الغرباء

إذا بدا أحد المرفقات داخل بريد إلكتروني مريباً، فلا تفتحه. لا تقم بتثبيت أي برنامج إلا إذا كان مصدره موقع إنترنت تثق به. وإذا كان لديك أي شك بهذا الخصوص، فيستحسن أن تأخذ كامل وقتك.

تعلم كيفية اكتشاف رسائل البريد الإلكتروني المزورة ومواقع الإنترنت المزيفة

يستخدم المجرمون رسائل إلكترونية مزورة ومواقع مزيفة. ويقومون بإعدادها لخداع الناس والحصول منهم على كلمات السر والمعلومات المصرفية. الكلمة التقنية لهذا هو «التصيد الاحتيالي».

على سبيل المثال، قد يرسل لك المجرمون بريداً إلكترونياً بحيث يبدو تماماً أنه من طرف البنك وقد يحتوي على رابط إلى موقع إنترنت يبدو كهذا. وعند محاولة تسجيل الدخول، سيمكنهم سرقة كلمة المرور الخاصة بك. وقد يطلبون منك القيام بإجراء مكالمة هاتفية أو الرد عن طريق البريد الإلكتروني.

أن مستواهم الجيد سيجعل رسائل البريد الإلكتروني ومواقع الإنترنت تبدو واقعية وحقيقية. ولكن، ورغم ذلك، سيمكنك في كثير من الأحيان تحديد الرسائل والمواقع المزيفة:

- شكل البريد الإلكتروني أو عناوين المواقع مبتذل أو غريب جداً
- تصميم سيئ، أخطاء مطبعية أو لغة بقواعد سيئة
- الطلب منك أن تفعل شيئاً غير عادي
- ألا يعرض الموقع «رمز القفل» في شريط العنوان عند تسجيل الدخول

تجنب الضغط على الروابط في رسائل البريد الإلكتروني. إن نقطة البداية في طريق حماية نفسك عبر الإنترنت هي وبرامج تصفح الإنترنت الحديثة المواقع Rapport استخدام البرنامج الذي نشير إليه من هذا الموقع. سيحظر برنامج المزيفة.

قمّ بحماية هاتفك المتحرك

قد يحتوي هاتفك المتحرك على معلومات شخصية

وقد يصادف أنك تستخدمه للدخول إلى الخدمات المصرفية عبر الإنترنت وللتسوق عبر الإنترنت.

فعلى سبيل المثال، قد يرسل لك المجرمون بريداً إلكترونياً بحيث يبدو تماماً أنه من طرف البنك الذي تتعامل معه وقد

يحتوي على رابط إلى موقع إنترنت يبدو كهذا. وعند محاولة تسجيل الدخول، سيمكنهم سرقة كلمة المرور الخاصة بك. قد يطلبون منك القيام بإجراء مكالمة هاتفية أو الرد عن طريق البريد الإلكتروني.

بعد ما ذكرناه سابقاً، قد ترغب في التفكير والقيام بـ:

على هاتفك المتحرك PIN ● إعداد واستخدام رمز التعريف الشخصي

● ضبط إعدادات الهاتف المتحرك بحيث يتم قفله تلقائياً إذا لم يتم إعادة استخدامه خلال مدة خمس أو عشر دقائق

● عدم القيام بحفظ كلمات المرور أو غيرها من المعلومات الحساسة على هاتفك بطريقة يمكن أن يفهمها أي شخص آخر

● عدم حفظ رقم هاتف منزلك وعنوانه تحت اسم «المنزل» في قائمة جهات الاتصال (فأنت بالطبع لا تريد أن يتمكن سارق الهاتف من معرفة عنوانك وأن يكون قادراً على التحقق مما إذا كنت في المنزل أو لا).

● التنبه والحذر من رسائل البريد الصوتي والرسائل النصية المزورة والاحتيالية

● عدم الضغط على الروابط في الرسائل النصية قبل التحقق من مرسليها، لأن هذا قد يكون محفوفاً بالمخاطر ـكن دائماً على حذر

الخاص IMEI إذا فقدت هاتفك، قم مباشرة بإبلاغ مزود الخدمة على هاتفك المتحرك بالسرقة. قم بتدوين رقم ال بهاتفك المتحرك (اطلب#06#* للحصول عليه)، لأن تقديمه لشركة مزود الخدمة سيسهل عملية تعطيل الهاتف المسروق.

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©