احمِ هويتك

نصائح للحفاظ على أمن هويتك

مكتب المدعي العام لولاية نيويورك
ليتيشا جيمس

المصادر

مكتب المدعي العام لولاية نيويورك، مكتب عمليات الاحتيال على المستهلكين

للإبلاغ عن عمليات الاحتيال أو رفع شكوى.

(800) 771-7755 / ag.ny.gov

لجنة التجارة الفيدرالية

للإبلاغ عن عمليات الاحتيال أو سرقة الهوية.

877- 382-4357 / ftc.gov

تقرير الائتمان

للتحقق من تقارير الائتمان أو تجميدها.

877-322-8228 / annualcreditreport.com

وكالات التقارير الائتمانية الرئيسية

Experian:
(888) 397-3742 / experian.com

TransUnion:
(800) 888-4213 / transunion.com

Equifax:
(800) 685-1111 / equifax.com

Innovis:
innovis.com

سكان نيويورك الأعزاء،

هويتك معرضة للخطر. عبر الإنترنت وعبر الهاتف وحتى شخصيًا، أصبح من السهل على المحتالين سرقة معلوماتك الشخصية واستخدامها لارتكاب عمليات الاحتيال أكثر من أي وقت مضى.

تؤثر سرقة الهوية على ملايين الأشخاص كل عام. يتقدم المحتالون بطلب للحصول على بطاقات ائتمان باسمك، ويحصلون على المزايا الطبية الخاصة بك، بل ويستخدمون رقم الضمان الاجتماعي الخاص بك للاحتيال الضريبي، مما يؤدي إلى إتلاف وضعك الائتماني وتكلفك الوقت والمال لإصلاحه.

يمكنك حماية معلوماتك الشخصية ومنع معظم أشكال سرقة الهوية بأقل جهد، ونحن هنا لمساعدتك في معرفة كيفية القيام بذلك.

لمزيد من التفاصيل حول كيفية الحفاظ على أمن هويتك، أو ما يجب فعله إذا كنت تعتقد أن هويتك قد سُرقت، يرجى الانتقال إلى موقعنا الإلكتروني ag.ny.gov.

وتفضلوا بقبول فائق الاحترام،

Letitia James

المدعي العام
لولاية نيويورك
ليتيشا جيمس

تأمين معلوماتك الشخصية

في حين أنه من الآمن عمومًا إعطاء اسمك أو رقم هاتفك، فإن إخبار أحدًا بتاريخ ميلادك أو رقم الضمان الاجتماعي أو أي أرقام حسابات قد يعرضك لسرقة هويتك. يجب أيضًا تجنب الكشف عن أي معلومات تستخدمها كإجابة "احتياطية" للمواقع الإلكترونية عندما تنسى كلمة مرور.

لا تعط معلوماتك الشخصية أبدًا إلى شخص يتصل بك بشكل عشوائي: إلا إذا كنت قد تواصلت معه، فهناك احتمال أنك تتعرض "للتصيد الاحتيالي".

التصيد الاحتيالي هو محاولة لجعل الضحية يقدم معلومات شخصية مثل اسم المستخدم أو كلمة المرور أو رقم بطاقة الائتمان الخاصة به. قد يتصل بك المحتالون عن طريق الرسائل النصية أو الهاتف أو البريد الإلكتروني، وغالبًا ما يتظاهرون بأنهم وكالة حكومية أو بنك أو شركة معروفة. سيطلبون معلوماتك الشخصية لحل بعض المشكلات أو حالات الطوارئ، أو يقولون إنهم بحاجة فقط إلى "تأكيد معلوماتك" قبل أن يتمكنوا من إعطائك شيئًا.

لن تتصل بك أي من هذه المؤسسات بهذه الطريقة للحصول على معلومات هامة. إذا لم تكن متأكدًا، فاتصل بالشركة - باستخدام الأرقام المعلنة - للتحقق من صحتها. تخبرك بعض محاولات التصيد الاحتيالي بالذهاب إلى موقع إلكتروني أو فتح مرفق. **لا تقم بتنزيل المرفقات أو تنقر على روابط من أشخاص لا تعرفهم.** فقد تحتوي على فيروسات تصيب جهاز الكمبيوتر الخاص بك وتسرق معلوماتك الشخصية.

الرسائل المشبوهة

حتى إذا ظهرت الرسالة كأنها واردة من مصدر موثوق به مثل أحد الأقارب أو الشركات المعروفة، فقد تظل محاولة تصيد احتيالي: ربما استولى المحتالون على الحساب أو أنشأوا حسابًا جديدًا يحمل اسمًا مشابهًا. إذا تلقيت رسالة لا تبدو مثل المرسل، أو تحتوي فقط على رابط أو مرفق بدون أي تفسير، أو تبدو مشبوهة بأي طريقة أخرى، فتحقق مرة أخرى من حقل "من" للتأكد من أنه العنوان الصحيح أو اتصل بالمرسل للتحقق من أنه حقًا هو. وقد يحدث هذا على وسائل التواصل الاجتماعي بنفس سهولة التعامل مع البريد الإلكتروني أو الرسائل النصية، لذا فلا تثق في أي رسالة مشبوهة لمجرد أنها تأتي من "صديق".

رقم الضمان الاجتماعي

لا يوجد أي داعٍ لشركة الضمان الاجتماعي الخاص بك. وإذا قامت شركة بذلك، فاسألهم عن سبب حاجتهم إليه، خاصة إذا لم تكن وكالة حكومية أو صاحب عمل أو مصرفًا أو مؤسسة مالية. **ومرة أخرى، لا تعطه أبدًا إلى شخص يتصل بك دون أن تطلبه.**

استخدام جدار حماية، تحديث نظام التشغيل

يمكن أن يؤدي تصفح الويب إلى تعريض جهاز الكمبيوتر للفيروسات. حافظ على تحديث نظام التشغيل وبرنامج مكافحة الفيروسات لديك وحافظ على تشغيل جدار الحماية للبقاء آمنًا.

إنشاء كلمات مرور قوية

إذا كنت تستخدم الإنترنت، فأنت بحاجة إلى كلمات مرور قوية، وتحتاج إلى العديد منها. كلمة المرور القوية تتسم بأنها:

- طويلة. يجب أن تتكون من ثمانية أحرف على الأقل، ولكن كلما زاد عدد الأحرف كان ذلك أفضل.
- لا يمكن أن يخمنها شخص يبحث عنك، لذلك لا أعياد ميلاد أو أسماء أقارب.
- كلمة مرور يمكنك تذكرها. يمكن أن يكون الجمع بين الكلمات الطويلة غير الشائعة ("batterystapler") مفيدًا هنا.
- تُستخدم مرة واحدة فقط. إذا كررت كلمة مرور وعرفها شخص ما مرة واحدة فيمكنه الوصول إلى جميع حساباتك.

مدراء كلمات المرور

المتصفحات الحديثة بها "مدراء كلمات مرور" يمكنك تثبيتها بحيث تتذكر كلمات المرور الخاصة بك: ما عليك سوى تنزيل أحد مدراء كلمات المرور وسيتم القيام بكل شيء آخر تلقائيًا. حافظ على أمان كلمة مرور مدراء كلمات المرور قدر الإمكان: إذا تمكن المحتال من الوصول إليها، فيمكنه الوصول إلى جميع حساباتك.

أجهزة حماية كلمات المرور

تعامل مع الهواتف الخلوية وحسابات الكمبيوتر تمامًا مثل الحسابات على المواقع الإلكترونية: امنحها كلمات مرور مميزة وقوية.

كلمات المرور الافتراضية

تأتي بعض الأجهزة، مثل جهاز الراوتر أو المودم، بكلمة مرور افتراضية. نادرًا ما تكون كلمات المرور الافتراضية آمنة، لذا يجب عليك تغييرها على الفور.

تغيير كلمات المرور بانتظام

حتى إذا كنت تتبع هذه النصيحة، فكلما طالت فترة استخدامك لكلمة المرور، زادت احتمالية حصول مخترق عليها: قد تتعرض المواقع الإلكترونية لخرق أمنها. قم دائمًا بتغيير كلمة المرور إذا تم اختراق الموقع الإلكتروني ذي الصلة، وقم بتغيير كلمات المرور بشكل دوري على أي حال للحفاظ على الأمان.

شبكات الاتصالات الآمنة

يمكن أن يكشف موقع ويب أو شبكة Wi-Fi غير آمنة معلوماتك الشخصية. لا تقم أبدًا بأعمال شخصية أو مالية على شبكة عامة، وتحقق للتأكد من أن موقع الويب "آمن" قبل منحه أي معلومات حساسة. ستبدأ المواقع الآمنة بـ **"https//:"** بدلاً من **"http//:"**

حذف البيانات غير الضرورية

دمّر أي سجلات للمعلومات الشخصية بمجرد عدم حاجتك إليها. مزّق المستندات المادية مثل الإيصالات والإقرارات الضريبية والسجلات المالية أو الطبية؛ احذف أو قم بإلغاء تنشيط الحسابات الرقمية واحذف الملفات الرقمية. تذكر أنه حتى الملفات المحذوفة يمكن أن تظل موجودة على محرك الأقراص الثابتة، لذا ستحتاج إلى برنامج أمان خاص لمسح جميع بياناتك الشخصية إذا كنت تتخلص من كمبيوتر قديم.

مراقبة الكشوفات

تحقق من كشوفات بطاقة الائتمان وكشوف الحسابات المصرفية بعناية بحثًا عن أي نشاط لم تصرح به.

تحقق بعناية من الفواتير الطبية والتأمين الصحي للتأكد من تلقيك العلاج الموضح.

تقارير الائتمان

يحق لكل فرد الحصول على نسخة مجانية واحدة من تقريره الائتماني كل عام من كل وكالة من وكالات التقارير الائتمانية الرئيسية. إذا رأيت حسابات أو استفسارات لم تقم ببدأها أو لم تتعرف عليها، فقد يشير ذلك إلى أن شخصًا آخر يستخدم هويتك. يمكنك جدولة التقارير من وكالات مختلفة في أوقات مختلفة من العام للحصول على تغطية منتظمة على موقع annualcreditreport.com أو 322-8228 (877).

سرقة هوية الأطفال

هويات الأطفال هي الأكثر شيوعًا للسرقة، أحيانًا من قبل أفراد الأسرة ذوي التصنيفات الائتمانية السيئة. احم معلومات أطفالك الشخصية كما تفعل مع معلوماتك الشخصية. تأكد من طرح الأسئلة واتخاذ الإجراءات إذا تلقوا مكالمات لتحصيل الفواتير أو عروض ائتمان بأسمائهم، أو تم رفض المزايا لأن شخصًا آخر يستخدم أرقامهم، أو تلقوا إشعارات من مصلحة الضرائب حول الضرائب المستحقة.