পিরয় নিউ ইয়কর্বাসীগণ,

আপনার পরিচয় বিপদের মধেয় রয়েছে। অনলাইনে, ফোনে এবং এমনকি বয্কি্তগতভাবে, পর্তারকদের পক্ষে আপনার বয্কি্তগত তথয় চুরি করা এবং জালিয়াতির জনয় এটি বয্বহার করা আগের চেয়ে সহজ।

পরিচয় চুরি করা পর্তি বছর লক্ষ লক্ষ মানুষজনকে পর্ভাবিত করে। পর্তারকরা আপনার নামে কের্ডিট কাডের্র জনয় আবেদন করে, আপনার চিকিত্সা সুবিধাগুলি গর্হণ করে এবং এমনকি আপনার সামাজিক সুরক্ষা নমব্রটি কর জালিয়াতির জনয় বয্বহার করে, আপনার ঋণের স্থিতিকে ক্ষতিগর্স্থ করে এবংসমাধান করার জনয় সময় এবং অথর্ বয্য় করে।

আপনি আপনার বয্কি্তগত তথয় রক্ষা করতে পারেন এবং পরিচয় চুরির বেশিরভাগ রূপে অল্প মনোযোগ দিয়ে পর্তিরোধ করতে পারেন এবং কীভাবে তা করবেন সেটি শেখার জনয় আপনাকে সহায়তা করতে আমরা এখানে আছি।

কীভাবে আপনার পরিচয় সুরক্ষিত রাখা যায় বা আপনার পরিচয়টি চুরি হয়ে গেছে এই বিষয়ে আপনি বিশব্াস করলে সেইক্ষেতের্ কী করবেন সে সম্পকের্ আরও বিস্তারিত বিবরণের জনয় অনুগর্হ করে আমাদের ওয়েবসাইট ag.ny.gov-এ যান।

বিনীত,

Letitia James

অয্াটর্নি জেনারেল অব নিউ ইয়কর্ লেটিশিয়া জেমস

সংস্থানসমূহ

New York State অয্াটর্নি জেনারেল কনজিউমার ফর্ড বুয্রোর অফিস

স্কয্াম রিপোর্ট করুন বা অভিযোগ জমা করুন।

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

মার্কিন যুক্তরাষ্ট্রীয় ফেডারেল টের্ড কমিশন

স্কয্াম বা পরিচয় চুরি রিপোর্ট করুন।

877- 382-4357 / ftc.gov

ঋণের বার্ষিক পর্তিবেদন

আপনার কের্ডিটের রিপোর্ট দেখার বা থামিয়ে দেওয়ার জনয়।

877-322-8228 / annualcreditreport.com

ঋণের পর্তিবেদন পর্স্তুতকারী পর্ধান এজেন্সিসমূহ

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

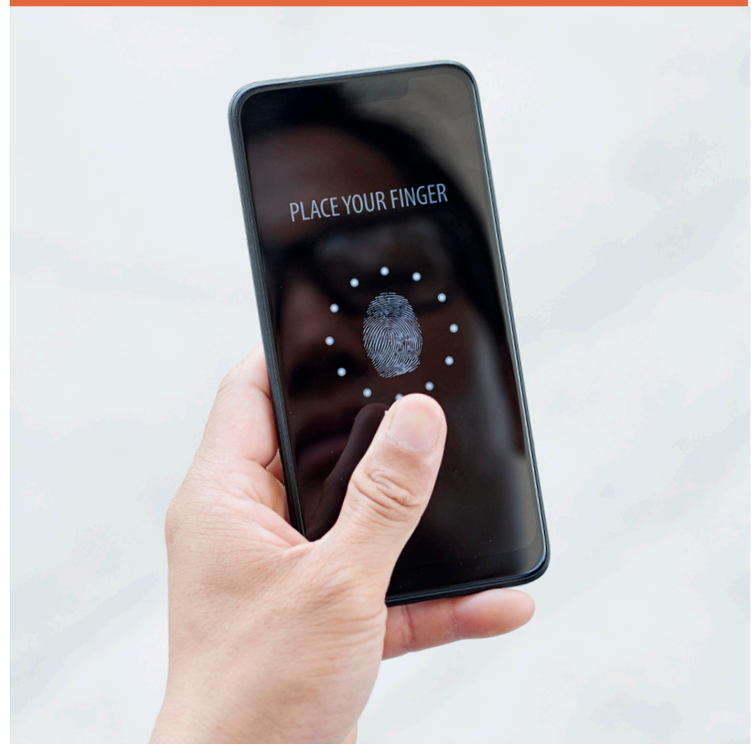
TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

আপনার পরিচয় সুরক্ষিত করুন

আপনার পরিচয় নিরপপদ রাখতে টিপস



নিউ ইয়কর্ স্টেট এর অয্াটর্নি জেনারেল লেটিশিয়া জেমস এর দপ্তর

আপনার বয্ক্তিগত তথয্ সুরক্ষিত করুন

আপনার নাম বা ফোন নমব্র কাউকে বলা নিরাপদ হলেও কাউকে আপনার জন্মতারিখ, সোশয্াল সিকিউরিটি নমব্র বা যে কোনো অয্াকাউন্ট নমব্র বললে আপনি বিপদের মুখে পড়তে পারেন। আপনি যখন পাসওয়াড্র ভুলে যান তখন ওয়েবসাইটগুলির জনয্ "বয্াকআপ" উত্তর হিসাবে আপনি যে তথয্ বয্বহার করেন তা পর্কাশ করাও এড়ানো উচিত।

কোনো বয্ক্তি আপনার সাথে এলোমেলোভাবে যোগাযোগ করলে তাকে কখনই আপনার বয্ক্তিগত তথয্ দেবেন না: যদি না আপনি তাদের সাথে নিজে থেকে যোগাযোগ করে থাকেন, কারণ সেক্েষতের্ আপনার "ফিশড" হওয়ার সম্ভাবনা রয়েছে।

ফিশিং হচ্েছ একজন কষতিগর্স্ত বয্ক্তির থেকে তার ইউজারনেম, পাসওয়াড্র, বা কের্ডিট কাড্র নমব্রের মতো বয্ক্তিগত তথয্ নেওয়ার চেষ্টা করা। স্কয্ামাররা টেক্সট, ফোন বা ইমেইলের মাধয্মে আপনার সাথে যোগাযোগ করতে পারে এবং পর্ায়শই একটি সরকারি সংস্থা, বয্াংক বা সুপরিচিত কোম্পানি হিসেবে নিজেদের পরিচয় দিতে পারে। কিছু সমসয্া বা জরুরী কোনো ঘটনার সমাধানের জনয্ তারা আপনার বয্ক্তিগত তথয্ দাবি করবে, অথবা তারা বলবে যে তাদের "আপনার কিছু তথয্ নিশ্চিত করতে হবে" যাতে তারা আপনাকে কিছু পর্দান করতে পারে।

এই সংস্থাগুলি কখনই আপনাকে কোনো গুর্ত্বপূণর্ তথেয্র জনয্ এইভাবে যোগাযোগ করবে না। যদি আপনার সন্েদহ থাকে, তাহলে কোম্পানিকে কল করুন - তাদের পর্কাশিত নমব্রে - এটি আসলে তারা কিনা তা যাচাই করতে। কিছু ফিশিং পর্চেষ্টা আপনাকে একটি ওয়েবসাইটে যেতে বা একটি অয্াটাচমেন্ট খুলতে বলে। অপরিচিত কারো থেকে পাওয়া কোনো অয্াটাচমেন্ট ডাউনলোড করবেন না বা তাদের থেকে পাওয়া কোনো লিঙ্েক কিলক করবেন না। এর মধেয্ এমন ভাইরাস থাকতে পারে যা আপনার কম্পিউটারের ক্ষতি করবে এবং আপনার বয্ক্তিগত তথয্ চুরি করবে।

সন্েদহজনক মেসেজ

এমনকি যদি কোনো আত্মীয় বা পরিচিত কোম্পানির মতো বিশব্স্ত উত্স থেকে কোনো মেসেজ আসে বলে মনে হয়, তবুও এটা একটা ফিশিং পরচেষ্টা হতে পারে: স্কয্ামাররা হয়তো ইতোমধেয্ অয্াকাউন্টটি দখল করে নিয়েছে অথবা একই নামের একটি নতুন অয্াকাউন্ট তৈরি করেছে। যদি আপনি এমন কোন মেসেজ পান যা সঠিক পের্রকের থেকে এসেছে বলে আপনি মনে করেন না, কোন বয্াখয্া ছাড়াই কেবল একটি লিঙ্ক বা অয্াটাচমেন্ট আছে, অথবা অনয্থায় সন্েদহজনক বলে মনে হয়, সঠিক ঠিকানার জনয্ 'ফর্ম' ফিল্ডটা যাচাই করুন বা পের্রককে কল করে এটা যাচাই করুন। এটি সোশয্াল মিডিয়ার সাথে সাথে খুব সহজেই ইমেইল বা টেকসটের মাধয্মে ঘটতে পারে, তাই সন্েদহজনক কোনো মেসেজ আপনার "বন্ধু"-এর থেকেই এসেছে বলে বিশব্াস করবেন না।

• আপনার সোশয্াল সিকিউরিটি নমব্র

আপনার সোশয্াল সিকিউরিটি নমব্র কোনো কোম্পানির জনয্ খুবই কম পর্য়োজন হয়। যদি পর্য়োজন হয়, জিজ্ঞাসা করুন কেন সেটার পর্য়োজন, বিশেষত সেটা যদি কোনো সরকারী সংস্থা, আপনার নিয়োগকতর্া, বয্াঙ্ক বা আথির্ক পর্তিষ্ঠান হয়। এবং আবার, কখনই এমন কাউকে দেবেন না, যে আপনাকে আপনার অপর্য়োজনে কল করেছে।

ফায়ারওয়াল বয্বহার করুন, আপনার অপারেটিং সিস্েটম আপডেট করুন

ওয়েব বর্াউজ করলে আপনার কম্পিউটারকে ভাইরাসের ঝুঁকিতে ফেলতে পারে। আপনার অপারেটিং সিস্েটম এবং অয্ান্টিভাইরাস পের্াগর্াম আপডেট রাখুন এবং নিরাপদ থাকার জনয্ আপনার ফায়ারওয়াল চালু রাখুন।

পোক্ত পাসওয়াড্র বয্বহার করুন;

আপনি যদি ইন্টারনেট বয্বহার করেন, আপনার পোক্ত পাসওয়াড্র পর্য়োজন হয়, এবং আপনার সেগুলির বেশ কয়েকটি পর্য়োজন। একটি পোক্ত পাসওয়াড্র হল:

- যে দীঘর্ হবে। সেটি কমপক্েষ আটটি কয্ারেক্টারের হবে, যত বেশি তত ভাল।.
- আপনার বয্াপারে তথয্ সংগর্হ করছে এমন কেউ অনুমান করতে পারবে না, তাই জন্মদিন বা আত্মীয়র নাম বাদ রাখুন।
- যেটা আপনি মনে রাখতে পারবেন। দীঘর্, সচরাচর বয্বহার করা হয় না এমন শব্েদর ("বয্াটারিস্টয্াপলার") মিশর্ণ এখানে উপকারী হতে পারে।
- কেবল একবার বয্বহার করা হবে। যদি আপনি একটি পাসওয়াড্র পুনরাবৃত্তি করেন এবং কেউ একবার এটি শিখে নেয় তবে তারা আপনার সমস্ত অয্াকাউন্েটর অয্াক্েসস পেতে পারে।

পাসওয়াড্র মযা্নেজার

আধুনিক বর্াউজারে "পাসওয়াড্র মযা্নেজার" থাকে যা আপনি ইনস্টল করতে পারবেন এবং যা আপনার জনয্ আপনার পাসওয়াড্র মনে রাখে: কেবল একটি পাসওয়াড্র মযা্নেজার ডাউনলোড করুন এবং অনয্ সবকিছু সব্য়ংকির্য়ভাবে সম্পন্ন হবে। আপনার পাসওয়াড্র মযা্নেজারের পাসওয়াড্র যথাসম্ভব সুরক্ষিত রাখুন: যদি কোন স্কয্ামার এতে অয্াক্েসস পায় তবে তারা আপনার সমস্ত অয্াকাউন্ট অয্াক্েসস করতে পারবে।

পাসওয়াড্র দব্ারা সুরক্ষিত ডিভাইস

সেল ফোন এবং কম্পিউটারের অয্াকাউন্টগুলিকে একটি ওয়েবসাইটের অয্াকাউন্েটর মতো বিবেচনা করুন: তাতে অননয্, পোক্ত পাসওয়াড্র দিন।

ডিফল্ট পাসওয়াড্র

কিছু ডিভাইস, যেমন আপনার রাউটার বা মডেমে, একটি ডিফল্ট পাসওয়াড্র থাকে। ডিফল্ট পাসওয়াড্রগুলি খুব কম সময়ই সুরক্ষিত থাকে, তাই আপনার অবিলমেব্ সেগুলির পরিবতর্ন করা উচিত।

নিয়মিত পাসওয়াড্র পরিবতর্ন করুন

এমনকি যদি আপনি এই পরামশর্টি অনুসরণ করেন, আপনি যত দীঘর্ সময় একই পাসওয়াড্র বয্বহার করবেন আপনার পাসওয়াড্র কোনো অসত্ বয্ক্তির হাতে পরে যাওয়ার সমভাবনা তত বেশি হবে: ওয়েবসাইটের নিরাপত্তা লঙ্ঘন হতে পারে। যদি ওয়েবসাইটের নিরাপত্তা লঙ্ঘন হয় তবে অবিলমেব্ পাসওয়াড্র পরিবতর্ন করুন এবং নিরাপদ থাকার জনয্ সময় সময় পাসওয়াড্র পরিবতর্ন করুন।

সংযোগ সুরক্ষিত রাখুন

একটি অ-সুরক্ষিত ওয়েবসাইট বা ওয়াই-ফাই নেটওয়াকর্ আপনার বয্ক্তিগত তথয্ পর্কাশ করতে পারে। কোনো পাবলিক নেটওয়াকের্ কখনোই বয্ক্তিগত বা আথির্ক বয্বসা পরিচালনা করবেন না এবং কোনো ওয়েবসাইটে গুর্ত্বপূণর্ কিছু দেওয়ার আগে তা "নিরাপদ" কিনা তা যাচাই করে নিন। সিকিওর করা ওয়েবসাইগুলি শুরু হবে **"https://"** দিয়ে এটির পরিবতের্ **"http://"**

অপর্য়োজনীয় ডেটা মুছুন

বয্ক্তিগত তথেয্র যে কোনো রেকড্র আপনার আর পর্য়োজন না হলে তা নষ্ট করে ফেলুন। রসিদ, টয্াক্স রিটানর্, এবং আথির্ক বা মেডিকেল রেকড্েরর মতো পর্কৃত নথি ছিঁড়ে ফেলুন; ডিজিটাল অয্াকাউন্ট মুছে ফেলুন বা নিষ্িকর্য় করুন এবং ডিজিটাল ফাইল মুছে ফেলুন। মনে রাখবেন যে মুছে ফেলা ফাইলগুলিও আপনার হাড্র ড্রাইভে বিদযমান থাকতে পারে, তাই আপনার পুরানো কম্পিউটার ফেলে দেওয়ার আগে আপনার সমস্ত বয্ক্তিগত ডেটা মুছে ফেলার জনয্ আপনার বিশেষ নিরাপত্তা সফ্টওয়য্ার পর্য়োজন।

বিবৃতির পযর্বেক্ষণ করুন

আপনি অনুমোদিত নয় এমন কোনও কির্য়াকলাপের জনয্ কের্ডিট কাড্র এবং বয্াঙ্ক স্েটটমেন্ট সাবধানে যাচাই করুন।

বর্ণির্ত চিকিত্সা আপনি পর্কৃতরূপে পেয়েছেন কিনা তা নিশ্চিত করার জনয্ মেডিকাল বিল এবং সব্াস্থয্ বীমা সাবধানে যাচাই করুন।

কের্ডিটের রিপোটর্

পর্তেয্কেই পর্তি বছর পর্ধান কের্ডিট রিপোটির্ং এজেন্সি থেকে তাদের কের্ডিট রিপোটের্র একটি বিনামূলেয্ কপি পাওয়ার অধিকারী। আপনি যদি এমন অয্াকাউন্ট বা জিজ্ঞাসা দেখেন যা আপনার দব্ারা করা নয় বা আপনি চিনতে পারছেন না, তাহলে এটি ধারণা করা যেতে পারে যে অনয্ কেউ আপনার পরিচয় বয্বহার করছে। annualcreditreport.com or (877) 322-8228 -এ নিয়মিত কভারেজ পেতে বছরের বিভিন্ন সময়ে আপনি বিভিন্ন সংস্থার রিপোটর্ পেতে পারেন।

শিশু পরিচয় চুরি

শিশুদের পরিচয় সবচেয়ে বেশি চুরি হয়ে যায়, কখনও কখনও পরিবারের সদসয্রা যাদের খারাপ কের্ডিট রেটিং থাকে তারাই অপরাধী হন। আপনার সন্তানের বয্ক্তিগত তথয্ আপনার নিজের মতো করে সুরক্ষিত করুন। যদি আপনার শিশুর নামে বিল সংগর্হের কল আসে বা তারা কের্ডিট অফার পান, তাদের সুবিধাগুলি অসব্ীকার করা হয় কারণ অনয্ কেউ তাদের নমব্র বয্বহার করছে, বা তাদের নামে IRS থেকে বকেয়া করের নোটিশ আসে, তবে পর্শ্ন জিজ্ঞাসা করতে ভুলবেন না এবং যথাযথ পদক্েষপ নিন।