



অ্যাটর্নির্ জেনারেল
অব নিউ ইয়র্ক
লেটিশিয়া জেমস

পির্য় নিউ ইয়র্কবাসীগণ,

আপনার পরিচয় বিপদের মধ্যে রয়েছে। অনলাইনে, ফোনে এবং এমনকি বয়ক্টিগতভাবে, পর্তারকদের পক্ষে আপনার বয়ক্টিগত তথ্ চুরি করা এবং জালিয়াতির জন্ এটি বয়বহার করা আগের চেয়ে সহজ।

পরিচয় চুরি করা পর্তি বছর লক্ষ লক্ষ মানুষজনকে পর্তাবিত করে। পর্তারকরা আপনার নামে কের্ডিট কাডের জন্ আবেদন করে, আপনার চিকিত্সা সুবিধাগুলি গ্রহণ করে এবং এমনকি আপনার সামাজিক সুরক্ষা নম্বরটি কর জালিয়াতির জন্ বয়বহার করে, আপনার ঋণের স্থিতিকে কষতিগ্রস্থ করে এবংসমাধান করার জন্ সময় এবং অর্থ বয় করে।

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

কীভাবে আপনার পরিচয় সুরক্টিত রাখা যায় বা আপনার পরিচয়টি চুরি হয়ে গেছে এই বিষয়ে আপনি বিশ্বাস করলে সেইক্ষেতের কী করবেন সে সম্পকের আরও বিস্তারিত বিবরণের জন্ অনুগ্রহ করে আমাদের ওয়েবসাইট ag.ny.gov-এ যান।

বিনীত,
Letitia James

সংস্থানসমূহ

New York State অ্যাটর্নির্ জেনারেল কনজিউমার ফর্ড বুয়রোর অফিস

স্কয়াম রিপোর্টর্ করুন বা অভিযোগ জমা করুন।

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

মাকির্ন যুক্তরাষ্ট্রীয় ফেডারেল টের্ড কমিশন স্কয়াম বা পরিচয় চুরি রিপোর্টর্ করুন।

877-382-4357 / ftc.gov

ঋণের বায়র্ক পর্তিবেদন

আপনার কের্ডিটের রিপোর্টর্ দেখার বা থামিয়ে দেওয়ার জন্।

877-322-8228 / annualcreditreport.com

ঋণের পর্তিবেদন পর্স্তুতকারী পর্তান এজেন্সিসমূহ

Experian:

(888) 397-3742 / experian.com

TransUnion:

(800) 888-4213 / transunion.com

Equifax

(800) 685-1111 / equifax.com

Innovis

innovis.com



আপনার পরিচয় সুরক্টিত করুন

আপনার পরিচয় নিরপদ রাখতে টিপস



নিউ ইয়র্ক স্টেট এর অ্যাটর্নির্
জেনারেল লেটিশিয়া জেমস এর
দপ্তর

আপনার বয়ক্‌তগত তথ্য্‌ সুরক্‌ষত করুন

আপনার নাম বা ফোন নমব্র‌র কাউকে বলা নিরাপদ হলেও কাউকে আপনার জন্মতারিখ, সোশ্যাল সিকিউরিটি নমব্র‌র বা যে কোনো অ্যাকাউন্ট নমব্র‌র বললে আপনি বিপদের মুখে পড়তে পারেন। আপনি যখন পাসওয়াড্‌র ভুলে যান তখন ওয়েবসাইটগুলির জন্য্‌ “বয়ক্‌আপ” উত‌র হিসাবে আপনি যে তথ্য্‌ বয়বহার করেন তা প্রকাশ করাও এড়ানো উচিত।

কোনো বয়ক্‌িত আপনার সাথে এলোমেলোভাবে যোগাযোগ করলে তাকে কখনই আপনার বয়ক্‌িতগত তথ্য্‌ দেবেন না: যদি না আপনি তাদের সাথে নিজে থেকে যোগাযোগ করে থাকেন, কারণ সেক্ষেত্রে আপনার “ফিশড” হওয়ার সম্ভাবনা রয়েছে।

ফিশিং হচ্ছে একজন কয়তিগরস্‌ত বয়ক্‌িতর থেকে তার ইউজারনেম, পাসওয়াড্‌র, বা কের্‌ডিট কার্ড‌র নমব্র‌রের মতো বয়ক্‌িতগত তথ্য্‌ নেওয়ার চেষ্টা করা। স্ক্যামাররা টেকসট, ফোন বা ইমেইলের মাধ্যমে আপনার সাথে যোগাযোগ করতে পারে এবং পরায়ুষই একটি সরকারি সংস্থা, বয়ংক বা সুপরিচিত কোম্পানি হিসেবে নিজেদের পরিচয় দিতে পারে। কিছু সমসয়া বা জরুরী কোনো ঘটনার সমাধানের জন্য তারা আপনার বয়ক্‌িতগত তথ্য্‌ দাবি করবে, অথবা তারা বলবে যে তাদের “আপনার কিছু তথ্য্‌ নিশ্চিত করতে হবে” যাতে তারা আপনাকে কিছু পরদান করতে পারে।

এই সংস্থাগুলি কখনই আপনাকে কোনো গুরুতব্পূর্ণ তথেষর জন্য্‌ এইভাবে যোগাযোগ করবে না। যদি আপনার সনেদহ থাকে, তাহলে কোম্পানিকে কল করুন - তাদের প্রকাশিত নমব্র‌র - এটি আসলে তারা কিনা তা যাচাই করতে। কিছু ফিশিং প্রচেষ্টা আপনাকে একটি ওয়েবসাইটে যেতে বা একটি অ্যাটাচমেন্ট খুলতে বলে। অপরিচিত কারো থেকে পাওয়া কোনো অ্যাটাচমেন্ট ডাউনলোড করবেন না বা তাদের থেকে পাওয়া কোনো লিঙ্ক ক্লিক করবেন না। এর মধ্যে এমন ভাইরাস থাকতে পারে যা আপনার কম্পিউটারের ক্‌ষতি করবে এবং আপনার বয়ক্‌িতগত তথ্য্‌ চুরি করবে।

সনেদহজনক মেসেজ

এমনকি যদি কোনো আতমীয় বা পরিচিত কোম্পানির মতো বিশ্বস্‌ত উত্‌স থেকে কোনো মেসেজ আসে বলে মনে হয়, তবুও এটা একটা ফিশিং প্রচেষ্টা হতে পারে: স্ক্যামাররা হয়তো ইতোমধ্যে অ্যাকাউন্টটি দখল করে নিয়েছে অথবা একই নামের একটি নতুন অ্যাকাউন্ট তৈরি করেছে। যদি আপনি এমন কোন মেসেজ পান যা সঠিক পের্রকের থেকে এসেছে বলে আপনি মনে করেন না, কোন বয়্যথ্যা ছাড়াই কেবল একটি লিঙ্ক বা অ্যাটাচমেন্ট আছে, অথবা অনযথায় সনেদহজনক বলে মনে হয়, সঠিক ঠিকানার জন্য ‘ফর্‌ম’ ফিল্ডটা যাচাই করুন বা পের্রককে কল করে এটা যাচাই করুন। এটি সোশ্যাল মিডয়ার সাথে সাথে খুব সহজেই ইমেইল বা টেকসটের মাধ্যমে ঘটতে পারে, তাই সনেদহজনক কোনো মেসেজ আপনার “বন্ধু”-এর থেকেই এসেছে বলে বিশ্বাস করবেন না।

• আপনার সোশ্যাল সিকিউরিটি নমব্র‌র

আপনার সোশ্যাল সিকিউরিটি নমব্র‌র কোনো কোম্পানির জন্য খুবই কম প্রয়োজন হয়। যদি প্রয়োজন হয়, জিজ্ঞাসা করুন কেন সেটার প্রয়োজন, বিশেষত সেটা যদি কোনো সরকারী সংস্থা, আপনার নিয়োগকর্তা, বয়ংক বা আর্থিক প্রতিষ্ঠান হয়। এবং আবার, কখনই এমন কাউকে দেবেন না, যে আপনাকে আপনার অপ্রয়োজনে কল করেছে।

ফায়ারওয়াল বয়বহার করুন, আপনার অপারেটিং সিস্টেম আপডেট করুন

ওয়েব বরাউজ করলে আপনার কম্পিউটারকে ভাইরাসের ঝুঁকিতে ফেলতে পারে। আপনার অপারেটিং সিস্টেম এবং অ্যানিটভাইরাস পেরাগরাম আপডেট রাখুন এবং নিরাপদ থাকার জন্য আপনার ফায়ারওয়াল চালু রাখুন।

পোকত পাসওয়াড্‌র বয়বহার করুন;

আপনি যদি ইন্টারনেট বয়বহার করেন, আপনার পোকত পাসওয়াড্‌র প্রয়োজন হয়, এবং আপনার সেগুলির বেশ কয়েকটি প্রয়োজন। একটি পোকত পাসওয়াড্‌র হল:

- যে দীঘল হবে। সেটি কমপক্ষে আটটি ক্যারেক্টারের হবে, যত বেশি তত ভাল।
- আপনার বয়্যপারে তথ্য্‌ সংগরহ করছে এমন কেউ অনুমান করতে পারবে না, তাই জন্মদিন বা আত্মীয়র নাম বাদ রাখুন।
- যেটা আপনি মনে রাখতে পারবেন। দীঘল, সচরাচর বয়বহার করা হয় না এমন শব্দ‌র (“ব্যাটারিস্ট্যাপনার”) মিশরণ এখানে উপকারী হতে পারে।
- কেবল একবার বয়বহার করা হবে। যদি আপনি একটি পাসওয়াড্‌র পুনরাব্‌তি করেন এবং কেউ একবার এটি শিখে নেয় তবে তারা আপনার সমস্‌ত অ্যাকাউন্ট‌র অ্যাক্‌সেস পেতে পারে।

পাসওয়াড্‌র ময়ানেজার

আধুনিক বরাউজারে “পাসওয়াড্‌র ময়ানেজার” থাকে যা আপনি ইনস্টল করতে পারবেন এবং যা আপনার জন্য আপনার পাসওয়াড্‌র মনে রাখে: কেবল একটি পাসওয়াড্‌র ময়ানেজার ডাউনলোড করুন এবং অন্য সবকিছু স্বয়ংকিয়ভাবে সম্পন্ন হবে। আপনার পাসওয়াড্‌র ময়ানেজারের পাসওয়াড্‌র যথাসম্ভব সুরক্‌ষত রাখুন: যদি কোন স্ক্যামার এতে অ্যাক্‌সেস পায় তবে তারা আপনার সমস্‌ত অ্যাকাউন্ট অ্যাক্‌সেস করতে পারবে।

পাসওয়াড্‌র দ্বারা সুরক্‌ষত ডিভাইস

সেল ফোন এবং কম্পিউটারের অ্যাকাউন্টগুলিকে একটি ওয়েবসাইট‌র অ্যাকাউন্ট‌র মতো বিবেচনা করুন: তাতে অনন্য, পোকত পাসওয়াড্‌র দিন।

ডিফল্ট পাসওয়াড্‌র

কিছু ডিভাইস, যেমন আপনার রাউটার বা মডেমে, একটি ডিফল্ট পাসওয়াড্‌র থাকে। ডিফল্ট পাসওয়াড্‌রগুলি খুব কম সময়ই সুরক্‌ষত থাকে, তাই আপনার অবিলম্বে সেগুলির প্রিবতর্ন করা উচিত।

নিয়মিত পাসওয়াড্‌র প্রিবতর্ন করুন

এমনকি যদি আপনি এই পরামশর্‌টি অনুসরণ করেন, আপনি যত দীঘল সময় একই পাসওয়াড্‌র বয়বহার করবেন আপনার পাসওয়াড্‌র কোনো অস্‌ত বয়ক্‌িতর হাতে পরে যাওয়ার সম্ভাবনা তত বেশি হবে: ওয়েবসাইট‌র নিরাপত্‌তা লঙ্ঘন হতে পারে। যদি ওয়েবসাইট‌র নিরাপত্‌তা লঙ্ঘন হয় তবে অবিলম্বে পাসওয়াড্‌র প্রিবতর্ন করুন এবং নিরাপদ থাকার জন্য সময় সময় পাসওয়াড্‌র প্রিবতর্ন করুন।

সংযোগ সুরক্‌ষত রাখুন

একটি অ-সুরক্‌ষত ওয়েবসাইট বা ওয়াই-ফাই নেটওয়ার্ক আপনার বয়ক্‌িতগত তথ্য্‌ প্রকাশ করতে পারে। কোনো পাবলিক নেটওয়ার্ক‌ে কখনোই বয়ক্‌িতগত বা আর্থিক বয়বসা পরিচালনা করবেন না এবং কোনো ওয়েবসাইটে গুরুতব্পূর্ণ কিছু দেওয়ার আগে তা “নিরাপদ” কিনা তা যাচাই করে নিন। সিকিওর করা ওয়েবসাইটগুলি শুরু হবে “https://” দিয়ে এটির প্রিবতর্ “http://”

অপ্রয়োজনীয় ডেটা মুছুন

বয়ক্‌িতগত তথেষর যে কোনো রেকড্‌র আপনার আর প্রয়োজন না হলে তা নশ্‌ট করে ফেলুন। রসিদ, ট্যাক্স রিটার্ন, এবং আর্থিক বা মেডিকেল রেকডে‌রর মতো প্রক্‌ত নথি ছিড়ে ফেলুন; ডিজিটাল অ্যাকাউন্ট মুছে ফেলুন বা নিশ্‌কিয় করুন এবং ডিজিটাল ফাইল মুছে ফেলুন। মনে রাখবেন যে মুছে ফেলা ফাইলগুলিও আপনার হার্ড ডরাইভে বিদ্যমান থাকতে পারে, তাই আপনার পুরানো কম্পিউটার ফেলে দেওয়ার আগে আপনার সমস্‌ত বয়ক্‌িতগত ডেটা মুছে ফেলার জন্য আপনার বিশেষ নিরাপত্‌তা সফ্‌টওয়ার প্রয়োজন।

বিব্‌তির প্রযর্‌বেক্‌ষণ করুন

আপনি অনুমোদিত নয় এমন কোনও কিয়াকলাপের জন্য কের্‌ডিট কার্ড্‌ এবং বয়ংক স্‌ট‌মেন্ট সাবধানে যাচাই করুন।

গণির্‌ত চিকিৎসা আপনি প্রক্‌তর্‌পে পেয়েছেন কিনা তা নিশ্‌চিত করার জন্য মেডিকাল বিল এবং স্বাস্‌থ্য বীমা সাবধানে যাচাই করুন।

কের্‌ডিট‌র রিপোর্ট্‌র

প্রতেযকেই প্রতি বছর প্রধান কের্‌ডিট রিপোর্টিং এজেনিস থেকে তাদের কের্‌ডিট রিপোর্ট‌রর একটি বিনাম্‌লেয় কপি পাওয়ার অধিকারী। আপনি যদি এমন অ্যাকাউন্ট বা জিজ্ঞাসা দেখেন যা আপনার দ্বারা করা নয় বা আপনি চিনতে পারছেন না, তাহলে এটি ধারণা করা যেতে পারে যে অন্য কেউ আপনার পরিচয় বয়বহার করেছে। annualcreditreport.com or (877) 322-8228 -এ নিয়মিত কভারেজ পেতে বছরের বিভিন্ন সময়ে আপনি বিভিন্ন সংস্থার রিপোর্ট্‌র পেতে পারেন।

শিশু পরিচয় চুরি

শিশুদের পরিচয় সবচেয়ে বেশি চুরি হয়ে যায়, কখনও কখনও পরিবারের সদস্যরা যাদের খারাপ কের্‌ডিট রেটিং থাকে তারাই অপরাধী হন। আপনার সন্তানের বয়ক্‌িতগত তথ্য্‌ আপনার নিজের মতো করে সুরক্‌ষত করুন। যদি আপনার শিশুর নামে বিল সংগর্‌হের কল আসে বা তারা কের্‌ডিট অফার পান, তাদের সুবিধাগুলি অস্বীকার করা হয় কারণ অন্য কেউ তাদের নমব্র‌র বয়বহার করেছে, বা তাদের নামে IRS থেকে বকেয়া করের নোটিশ আসে, তবে প্রর্‌শ্ন জিজ্ঞাসা করতে ভুলবেন না এবং যথযথ পদক্ষেপ নিন।