অবিলম্বে প্রকাশের উদ্দেশ্যে: 3/22/2022 **গভর্নর ক্যাথি হোকল**

গভর্নর হোকল ইউক্রেনে রাশিয়ান আক্রমণের মধ্যে ভোক্তাদের স্ক্যাম এবং সাইবার নিরাপত্তা হুমকির ব্যাপারে সতর্ক করলেন

দান করুন সত্যায়িত এবং নামকরা সংস্থাসমূহে যারা প্রাপ্ত সাহায্য অভাবী ইউক্রেনীয়দের ত্রাণ প্রদানে ব্যবহার করে

স্টেট এজেন্সিসমূহ আপনাদের সংবেদনশীল তথ্য সুরক্ষিত ও নিরাপদ রাখতে, বর্ধিত সাইবার হুমকির সময় সতর্ক থাকতে সুপারিশ জারি করছে

গভর্নর ক্যাথি হোকল আজকে নিউ ইয়র্কবাসীকে ভ্লাদিমির পুতিনের ইউক্রেন আক্রমণ সম্পর্কিত চ্যারিটি স্ক্যাম এবং সাইবার নিরাপত্তার বর্ধিত হুমকির ব্যাপারে পরামর্শ দান করেছেন। নিউ ইয়র্ক স্টেট ভোক্তা সুরক্ষা ডিভিশন (New York State Division of Consumer Protection) যুদ্ধের শিকার ব্যক্তিদের সমর্থনে দাতব্য ত্রাণের ভুয়া অনুরোধের ব্যাপারে জানতে পেরেছে। ভোক্তাদের অর্থের যেকোনও অনুরোধকে সাবধানে যাচাই করে দেখতে এবং অর্থ বা দ্রব্য দান করার পূর্বে চ্যারিটিকে যাচাই করে দেখতে উৎসাহিত করা হচ্ছে। এছাড়াও যেহেতু সাইবার নিরাপত্তা হুমকি বেড়ে যাচ্ছে তাই গভর্নর হোকল নিউ ইয়র্কবাসীদের অনলাইনে সংবেদনশীল তথ্য প্রকাশ করার পূর্বে কর ও অর্থ ডিপার্টমেন্টের (Department of Taxation and Finance) নিরাপত্তা সুপারিশসমূহ ব্যবহার করার মাধ্যমে সতর্ক হতে উৎসাহিত করেছেন। এটি গভর্নরের যৌথ নিরাপত্তা কর্মকাণ্ড কেন্দ্র (Joint Security Operations Center) গঠন করার অনুবর্তী, যা স্থানীয়, স্টেট এবং ফেডারেল সাইবার প্রচেষ্টার কেন্দ্র হিসেবে কাজ করে।

"নিউ ইয়র্ক মার্কিন যুক্তরাষ্ট্রের সর্ববৃহৎ ইউক্রেনীয় জনগোষ্ঠীর বাড়ি, এবং নিউ ইয়র্কবাসীরা সবসময় অভাবী সকলের দিকে সাহায্যের হাত বাড়িয়ে দেয়," **গভর্নর হোকল বলেন।** "কিন্তু, আমাদেরকে যারা অন্যদের উদারতার সুযোগ নিয়ে প্রতারণা করার চেষ্টা করে তাদের ব্যাপারে সতর্ক থাকতে হবে। আমাদের ইউক্রেনীয় বন্ধু ও পরিবারদের সাহায্য করতে আপনার দানশীলতার ক্ষেত্রে মনে রাখবেন যে, যদি কোনও কিছু সন্দেহজনক মনে হয় তাহলে এটি তাই হওয়াই স্বাভাবিক। আপনার বন্ধু ও পরিবারকে, বিশেষ করে বয়স্ক প্রিয়জনদের অনলাইনে সতর্ক থাকতে উৎসাহিত করুন।"

যেকোনও বিপর্যয় আসলে, স্ক্যামকারীরা সাহায্য করতে আগ্রহী ব্যক্তিদের উদারতার সুযোগ নিতে চায়। ইউক্রেনে আক্রমণ প্রতারণাকারীদের জন্য ভুয়া চ্যারিটি স্থাপন করা বা নিগৃহীত যুদ্ধের

শিকার ব্যক্তি হিসেবে ভান করার একটি সুযোগ প্রদান করছে। অন্যরা কোনও বৈধ চ্যারিটির আনুষ্ঠানিক সাইটের নকল করে ওয়েবসাইট ডিজাইন করে যাতে সরল বিশ্বাসী দাতাদের অর্থ এবং/অথবা ব্যক্তিগত তথ্য চুরি করতে পারে।

স্টেটের সচিব রবার্ট জে. রদ্রিগেজ বলেন, "নিউ ইয়র্কবাসীরা অভাবীদের প্রতি সমর্থক ও উদার হিসেবে পরিচিত। ইউক্রেনের যুদ্ধ যখন বেড়ে চলেছে, প্রতারণাকারীরা আবেগপূর্ণ ছলনা এবং ভুয়া অনুনয় ব্যবহার করে ভোক্তাদের সুযোগ নেওয়ার চেষ্টা অব্যাহতভাবে করছে। আমি নিউ ইয়র্কবাসীদের তাদের ভালো উদ্দেশ্য সুরক্ষিত রাখতে এবং কোনও চ্যারিটিতে দান করার পূর্বে সে ব্যাপারে জেনে নিতে উৎসাহিত করছি, যাতে এটি নিশ্চিত করতে পারেন যে আপনার কষ্টে উপার্জিত ডলার তাদের কাছেই যাচ্ছে যাদের আপনাদের সমর্থনের নিদারুণ প্রয়োজন রয়েছে।"

ভারপ্রাপ্ত কর এবং অর্থ কমিশনার আমান্ডা হিলার বলেন, "ইউক্রেনের বৈশ্বিক সঙ্কট সাইবার আক্রমণের উদ্বেগ বৃদ্ধি করেছে, তাই আমাদের সবাইকে অবশ্যই সতর্ক থাকতে হবে যাতে ভুল হাতে গোপন তথ্য চলে যাওয়া, সেবা দিতে অস্বীকার করে আক্রমণ, এবং অন্যান্য নেতিবাচক ফলাফল ঠেকানো যায়।"

তথ্য প্রযুক্তি অফিসের (Office of Information Technology Services, ITS) প্রধান তথ্য কর্মকর্তা অ্যাঞ্জেলো 'টনি' রিডিক বলেন, "অগণিত নিউ ইয়র্কবাসী ভালো উদ্দেশ্যে ইউক্রেনের মানুষদের সমর্থনের চ্যারিটিসমূহে দান করেছে, এবং তারা একটি পার্থক্য তৈরি করতে পারছে। দুর্ভাগ্যবশত, এই উদারতা সাইবার অপরাধীদের শোষণের জন্য নতুন সুযোগ সৃষ্টি করে। নিজেকে সুরক্ষা করার জন্য এবং আপনার উদার দান যাতে সর্বদা যাদের এর সবথেকে বেশি প্রয়োজন তাদের হাতেই পৌঁছায় তা নিশ্চিত করার জন্য, ITS নিউ ইয়র্কবাসীকে এই সেরা অনুশীলনসমূহ করতে বলছে এবং সাম্প্রতিক অনলাইন হুমকি ও সাইবার স্ক্যামের ঘটনার কারণে সতর্ক থাকতে বলছে।"

হোমল্যান্ড সিকিউরিটি এবং ইমারজেন্সি সার্ভিসেস ডিভিশনের (Division of Homeland Security and Emergency Services, DHSES) কমিশনার জ্যাকি ব্রে বলেন, "নিজেদের ব্যক্তিগত তথ্য নিরাপদ রাখার ক্ষেত্রে এবং নিজেদেরকে সাইবার হুমকি থেকে রক্ষা করার ক্ষেত্রে প্রত্যেক নিউ ইয়র্কবাসীর একটি ভূমিকা পালন করতে হবে। আমরা জানি অভাবের সময় খারাপ পক্ষরা যারা সাহায্য করতে চেষ্টা করছে তাদের সুযোগ নেওয়ার চেষ্টায় থাকে। আপনি যদি অনলাইন বা ডিজিটাল দানের মাধ্যমে ইউক্রেনের মানুষদের সমর্থন করতে চান, তাহলে সতর্ক থাকুন এবং আপনার দান খাঁটি এবং আপনার তথ্য নিরাপদ থাকা নিশ্চিত করতে এই সেরা অনুশীলনগুলি অনুসরণ করুন।"

স্টেটের সিনেটর কেভিন টমাস বলেন, "এতো বেশি নিউ ইয়র্কবাসী যে ইউক্রেনের মানুষকে সাহায্য করতে পদক্ষেপ নিয়েছে তা আমাদের প্রতিবেশীরা কেমন তা ভালোই বুঝিয়ে দেয়। দুর্ভাগ্যবশত, এটি স্ক্যামারদের জন্য ব্যক্তিগত স্বার্থে এই সঙ্কটের অপব্যবহার করার একটি বড় সুযোগ সৃষ্টি করেছে। আমি নিউ ইয়র্কবাসীদের সতর্ক থাকতে এবং তাদের উদার অবদান যাতে বৈধ কারণে খরচ হয় তা নিশ্চিত করতে অতিরিক্ত সতর্কতা গ্রহণ করার তাগিদ দিচ্ছি।"

অ্যাসেম্বলি সদস্য নাইলি রোজি বলেন, "স্ক্যামাররা সবসময় আপনাদের ধোঁকা দিতে নতুন নতুন পদ্ধতি চেষ্টা করে, এমনকি একটি আন্তর্জাতিক সঙ্কটের সময়েও। যখন ইউক্রেনের বিপদের সময় নিউ ইয়র্কবাসীরা তাদের সমর্থনে একত্রিত হয়েছে, তখন আপনার উদারতার অপব্যবহার যাতে না করা হয় তা নিশ্চিত করতে ভোক্তাদের দক্ষতা ও জ্ঞান প্রদান করা অত্যাবশ্যকীয়। নিউ ইয়র্কবাসীরা যাতে তাদের উদারতার জন্য স্ক্যামের শিকার না হয় তা নিশ্চিত করার জন্য আমি গভর্নর হোকলের প্রতি কৃতজ্ঞ।"

স্ক্যামাররা প্রায়শই সামাজিক যোগাযোগ মাধ্যম, অযাচিত ইমেইল, ফোন কল, বা টেক্সট বার্তার মাধ্যমে যোগাযোগ করে। তারা ক্যাশ অ্যাপ (Cash App), ভেনমো (Venmo) বা জেলের (Zelle) মতো পেমেন্ট অ্যাপের মাধ্যমে অর্থ চাইতে পারে, অফশোরের কোনও ব্যাংক অ্যাকাউন্টে অর্থ ওয়্যার করতে বলতে পারে, বা একটি প্রিপেইড গিফট কার্ড পাঠাতে বলতে পারে। সাম্প্রতিক অনেক স্ক্যামে বিটকয়েন (Bitcoin) বা এথেরিয়ামের (Ethereum) মতো ক্রিপ্টোকারেন্সি দানের অনুরোধ ছিলো। স্ক্যামকারীরা সৃজনশীল এবং মানুষকে প্রতারণা করতে নতুন নতুন পন্থা ভেবে বের করতে থাকবে, তাই ভোক্তাদের সর্বদা সতর্ক থাকতে হবে।

দানের অর্থ ভুল হাতে পৌঁছানো ঠেকাতে, নিউ ইয়র্ক স্টেট ভোক্তা সুরক্ষা ডিভিশন নিম্নোক্ত সতর্কতা অবলম্বন করার সুপারিশ দিচ্ছে:

- **অনুরোধ যাচাই করুন।** স্ক্যামাররা প্রায়ই সামাজিক যোগাযোগ মাধ্যমে বন্ধু, পরিবার বা সম্ভাব্য ভালোবাসার মানুষ সেজে দানের অনুরোধ করে; অনলাইনে কারো ছবি এবং জীবনসংক্রান্ত তথ্য নকল করে একটি ভুয়া অ্যাকাউন্ট তৈরি সহজ। আপনি যদি আপনার পরিচিত মনে হচ্ছে এমন কারো থেকেও অনলাইনে ত্রাণ দানের একটি অযাচিত অনুরোধ পান, তাহলে সেই ব্যক্তির সাথে একটি ভিন্ন যোগাযোগ ব্যবস্থায় সরাসরি যোগাযোগ করুন অনুরোধটি যাচাই করার জন্য। কোনও লিঙ্কে ক্লিক করবেন না বা উৎস যাচাই না করে কোনও ফর্ম পূরণ করবেন না। যদি অনুরোধটি এমন কারো থেকে আসে যার সাথে সম্প্রতি আপনার অনলাইনে পরিচয় হয়েছে, এটি খুব সম্ভবত একটি স্ক্যাম এবং আপনার বিশেষ ভাবে সতর্ক হওয়া উচিত।
- **চ্যারিটি নিয়ে রিসার্চ করুন।** শুধু চ্যারিটির ওয়েবসাইটের উপর নির্ভর করবেন না। কোনও চ্যারিটিতে দান করার পূর্বে গ্রুপের নাম ব্যবহার করে এবং "রিভিউ" এবং "স্ক্যাম" এ ধরনের সার্চ টার্ম লিখে অনলাইনে অনুসন্ধান করুন। ফেডারেল ট্রেড কমিশন (Federal Trade Commission) চ্যারিটির রিপোর্ট ও রেটিং দেখার জন্য give.org, charitynavigator.org,charitywatch.org বা candid.org দেখার সুপারিশ করছে। এছাড়াও আপনি ইন্টারনাল রেভেন্যু সার্ভিসে (Internal Revenue Service, IRS) দেখতে পারেন যে চ্যারিটিটি নিবন্ধিত কিনা। অ্যাটর্নি জেনারেলের অফিসও (Office of the Attorney General) দান করার পূর্বে চ্যারিটিটি আর্থিকভাবে সুপ্রতিষ্ঠিত কিনা তা নিশ্চিত করতে চ্যারিটিজ রেজিস্ট্রিতে আর্থিক রিপোর্ট দেখার সুপারিশ দিচ্ছে।
- **উচ্চ চাপের কৌশল প্রতিহত করুন।** যদিও পরিস্থিতিটি অতি জরুরি, কিন্তু ভোক্তাদের অবিলম্বে দান করার চাপ প্রতিহত করা উচিত। অনেক সময় স্ক্যামাররা আপনাকে

তাৎক্ষণিকভাবে দান করতে চাপ প্রদান করবে, যার ফলে আপনি তাদের গল্পের বিপদ সঙ্কেত দেখতে পাবেন না। হৃদয়গ্রাহী গল্প বলা "ভিকটিম" এবং সলিসিটরদের থেকে সরাসরি ইমেইল যেখানে আপনাকে তাৎক্ষণিকভাবে দান করতে বলা হয় সে ব্যাপারে সতর্ক হন। ফোন বা অযাচিত টেলিমার্কেটারদেরকে অর্থ দিবেন না, যে ফোন করেছে তাকে চ্যারিটির ব্যাপারে এবং কোথায় দান করতে হবে সে ব্যাপারে লিখিত জিনিষ পাঠাতে বলুন, যদি আপনি দিতে চান।

- **ব্যক্তিগত তথ্য গোপন রাখুন।** একটি অযাচিত চ্যারিটি অনুরোধের উত্তরে কখনো আপনার সোশ্যাল সিকিউরিটি নম্বর, ক্রেডিট কার্ড বা ডেবিট কার্ড তথ্য দিবেন না। অনলাইনে দান করার সময়, দানের অনুরোধ পূরণ করার পূর্বে নিশ্চিত করুন যে আপনার ইন্টারনেট সংযোগ নিরাপদ আছে।
- **প্রশ্ন করুন যে কীভাবে আপনার অর্থ ব্যয় করা হবে।** ভোক্তারা জানতে চায় যে তাদের অর্থ সরাসরি ভিকটিমদের কাছে যাচ্ছে। একটি খাঁটি চ্যারিটি আপনাকে জানাতে পারবে যে আপনার দানের কত অংশ প্রশাসনিক ফি হিসেবে ব্যবহৃত না হয়ে কর্মসূচিতে সরাসরি যাবে।

- **চেক বা ক্রেডিট কার্ড দিয়ে দান করুন।** কখনো নগদ, গিফট কার্ড, ক্রিপ্টো কারেন্সি, বা ট্রেস করতে কঠিন হবে এমন টেন্ডার দ্বারা অর্থ দিবেন না। আপনার কাছে দানের রেকর্ড আছে তা নিশ্চিত করতে চেক বা ক্রেডিট কার্ড দিয়ে অর্থ দান করুন। চেক লিখুন চ্যারিটির নামে, ব্যক্তির নামে নয়। আপনি যদি একটি চ্যারিটির ওয়েবসাইট দিয়ে দান করতে চান, তাহলে ওয়েবসাইটটি সুরক্ষিত কিনা এবং আপনার কম্পিউটারে সর্বশেষ অ্যান্টিভাইরাস সুরক্ষা রয়েছে কিনা দেখে নিন।

আপনি যদি সন্দেহ করেন যে দান পাওয়ার জন্য একটি ভুয়া চেষ্টার সম্মুখীন হয়েছেন, তাহলে আপনি নিউ ইয়র্ক স্টেট ভোক্তা সুরক্ষা ডিভিশনের কাছে অভিযোগ দায়ের করতে পারবেনhttps://dos.ny.gov/file-consumer-complaint।

ডিভিশনের ভোক্তা সহায়তা হটলাইন (Consumer Assistance Hotline) সোম থেকে শুক্রবার, সকাল 8:30 থেকে বিকাল 4:30 পর্যন্ত খোলা থাকে 1-800-697-1220 নম্বরে, স্টেটের সরকারি ছুটির দিন বাদে। আপনি আরো তথ্য ও পরামর্শ পেতে পারেন ভোক্তা সুরক্ষা ডিভিশনের সামাজিক যোগাযোগ মাধ্যম অনুসরণ করে, যা টুইটারে (@NYSConsumer)) এবং ফেসবুকে (www.facebook.com/nysconsumer)।

সাইবার নিরাপত্তার বর্ধিত আন্তর্জাতিক উদ্বেগের সময়, নিউ ইয়র্ক স্টেট কর ও অর্থ ডিপার্টমেন্ট এছাড়াও কর মৌসুমের সময় এবং পুরো বছরজুড়ে করদাতাদের ব্যক্তিগত তথ্য নিরাপদ রাখতে একাধিক অতি গুরুত্বপূর্ণ পরামর্শ প্রদান করেছে।

ব্যক্তিগত তথ্য চাওয়া অযাচিত ইমেইল ও ফোনের ব্যাপারে সতর্ক থাকুন। কখনো একটি অযাচিত ইমেইল বা টেলিফোন কলের উত্তরে সোশ্যাল সিকিউরিটি নম্বরের মতো ব্যক্তিগত তথ্য প্রদান করবেন না। যদি ইমেইল বা ফোনটি এমন কোনও কোম্পানি থেকে আসে যার সাথে

আপনি ব্যবসা করেন, তাহলে সরাসরি তাদের সাথে যোগাযোগ করে নিশ্চিত করুন যে যোগাযোগটি বৈধ ছিলো। স্ক্যামাররা প্রায়ই কর ঋণ সংক্রান্ত ভয় দেখানো কৌশল ও হুমকি ব্যবহার করে আপনার কাছ থেকে আপনার ব্যক্তিগত ও আর্থিক তথ্য পেয়ে যায়।

আপনার মোবাইল ডিভাইস নিরাপদ করুন। জানা দুর্বলতা ঠিক করে এমন সফটওয়্যার আপডেট উপলভ্য হওয়া মাত্র প্রয়োগ করুন। আপনার ডিভাইসের বিল্ট-ইন নিরাপত্তা ফিচার ব্যবহার করুন, যেমন একটি পাসকোড, এবং এমন প্রোগ্রাম ব্যবহার করুন যা ডেটা এনক্রিপ্ট করে এবং ফোন হারিয়ে গেলে বা চুরি গেলে দূর থেকে ফোনের সবকিছু মুছে দেয়।

ওয়াইফাই হটস্পট নিয়ে সাবধান হন। পাবলিক ওয়্যারলেস হটস্পট নিরাপদ নয়, যার অর্থ যে আপনি সংযুক্ত থকা অবস্থায় আপনি আপনার মোবাইল ডিভাইসে কী করছেন তা দেখা সাইবার চোরদের জন্য সহজ হয়ে যায়। পাবলিক ওয়াইফাইতে আপনার কাজ সীমিত করুন এবং সংবেদনশীল অ্যাকাউন্টে লগ ইন করা এড়িয়ে চলুন।

আপনার অ্যাপগুলি সম্পর্কে জানুন। কোনও অ্যাপ ডাউনলোড করার পূর্বে এর বিস্তারিত এবং স্পেসিফিকেশন ভালোভাবে রিভিউ করুন। প্রতি মোবাইল অ্যাপের গোপনীয়তা নীতিমালা রিভিউ করুন এবং বুঝে নিন। সচেতন থাকুন যে অ্যাপ আপনার অবস্থান এবং ব্যক্তিগত তথ্য জানতে চাইতে পারে।

আপনি সামাজিক যোগাযোগ মাধ্যমে কী তথ্য দিবেন সে ব্যাপারে সতর্ক থাকুন। আপনার জন্মতারিখ, টেলিফোন নম্বর, বাড়ির ঠিকানা বা আপনার চাকরি বা শখ সনাক্ত করে এমন ছবি পোস্ট করা থেকে এড়িয়ে চলুন। একটি কারণ: এটি ধরনের তথ্য পাসওয়ার্ড রিসেট করার নিরাপত্তা প্রশ্ন নির্ণয় করার জন্য ব্যবহার করা যেতে পারে, এবং ফলে আপনি আপনার অ্যাকাউন্ট ও ব্যক্তিগত তথ্য খুঁজছে এমন প্রতারকদের লক্ষ্য হয়ে যেতে পারেন।

শক্ত পাসওয়ার্ড ব্যবহার করুন। আপনার সকল অ্যাকাউন্টের জন্য ভিন্ন ভিন্ন পাসওয়ার্ড তৈরি করুন। পাসওয়ার্ডের ক্ষেত্রে, কমপক্ষে 14 অক্ষরের একটি ব্যবহার করার চেষ্টা করুন, যা বর্তমানে এ ক্ষেত্রে আদর্শ। অক্ষর (বড় হাতের এবং ছোট হাতের), সংখ্যা, এবং প্রতীকের একটি মিশ্রণ ব্যবহার করুন। পাসফ্রেজ ব্যবহার করতে পারেন যেখানে আপনি আপনি একটি স্মরণীয় ফ্রেজের প্রথম অক্ষরগুলি ব্যবহার করে একটি জটিল পাসওয়ার্ড তৈরি করতে পারবেন যা অনুমান করা কষ্ট। নিয়মিত আপনার পাসওয়ার্ড/পাসফ্রেজ পরিবর্তন করুন।

আপনার নিরাপত্তা প্রশ্নে তারতম্য রাখুন। একাধিক অ্যাকাউন্টে একই নিরাপত্তা প্রশ্ন ব্যবহার করবেন না। এমন নিরাপত্তা প্রশ্ন বাছাই করুন যার উত্তর অনুমান করা যাবে না বা সামাজিক যোগাযোগ মাধ্যম বা ইন্টারনেটে খুঁজে পাওয়া যাবে না।

অ্যাকাউন্ট ব্যবহার করার জন্য দুই ধাপের যাচাইকরণ ব্যবহার করুন। অনলাইন অ্যাকাউন্টসমূহের নিরাপত্তা উন্নত করতে, যখনই সম্ভব হবে তখনই আপনার সাইন ইন করার সময় আপনার পরিচয় যাচাইয়ের জন্য একটি পাসওয়ার্ড এবং একটি অতিরিক্ত নিরাপত্তা কোড আবশ্যক করুন।

ফিশিংয়ের ব্যাপারে সচেতন থাকুন। অপরিচিত প্রেরকের পাঠানো ইমেইলের লিঙ্ক, ডাউনলোড ফাইলে ক্লিক করবেন না বা অ্যাটাচমেন্ট খুলবেন না। প্রেরককে আপনি চিনলেও শুধু তখনই অ্যাটাচমেন্ট খুলুন যখন আপনি এর অপেক্ষা করছেন এবং জানেন এতে কী রয়েছে।

আপনার সংবেদনশীল তথ্য নিরাপদ করতে প্রয়োজনীয় ধাপ নিয়মিত পর্যালোচনা করা গুরুত্বপূর্ণsecure your sensitive information।

এটি রিপোর্ট করুন।আপনি যদি এর শিকার হয়ে থাকেন বা নিজেকে কর সম্পর্কিত পরিচয় চুরির শিকার বলে বিশ্বাস করেন, আমাদেরকে অবিলম্বে সে ব্যাপারে জানান। আমরা আপনার তথ্য ট্র্যাক করে তা গোপন ও সুরক্ষিত রাখতে সাহায্য করবো। কর ডিপার্টমেন্টের প্রতারণা, স্ক্যাম, এবং পরিচয় চুরি রিপোর্ট করার ওয়েবপেজটি ভিজিট করুন।

কর ডিপার্টমেন্ট (Tax Department) উন্নত এনক্রিপশন, ফায়ারওয়াল, অনধিকারপ্রবেশ-সনাক্তকরণ ব্যবস্থা, এবং অন্যান্য নিরাপত্তা ব্যবস্থা গ্রহণ করে আমাদের সিস্টেম এবং সংবেদনশীল ডেটা নিরাপদ রাখার জন্য, কিন্তু করদাতাদেরকেও নিজেদেরকে অনলাইনে সুরক্ষিত রাখতে একটি সক্রিয় পন্থা অবলম্বন করতে হবে।

###

আরো সংবাদ পাওয়া যাবে এখানে www.governor.ny.gov-এ
নিউ ইয়র্ক স্টেট | এক্সিকিউটিভ চেম্বার | press.office@exec.ny.gov | 518.474.8418