Diffusione immediata: 22/03/2022 **GOVERNATRICE KATHY HOCHUL**

LA GOVERNATRICE HOCHUL AVVERTE I CONSUMATORI SULLE TRUFFE E SULLE MINACCE ALLA SICUREZZA INFORMATICA A SEGUITO DELL'INVASIONE RUSSA DELL'UCRAINA

Dona a organizzazioni riconosciute e rinomate che usano i contributi per fornire aiuto agli ucraini in difficoltà

Le agenzie statali pubblicano raccomandazioni per proteggere e salvaguardare i tuoi dati sensibili, resta vigile in presenza di gravi minacce informatiche

La governatrice Kathy Hochul ha informato, oggi, i newyorkesi sulle truffe legate alla beneficenza e sull'aumento delle minacce alla sicurezza informatica collegate all'invasione dell'Ucraina da parte di Vladimir Putin. La Divisione per la protezione dei consumatori dello Stato di New York (New York State Division of Consumer Protection) è venuta a conoscenza di richieste fraudolente di aiuti di beneficenza per sostenere le vittime della guerra. I consumatori sono incoraggiati a valutare attentamente qualsiasi richiesta di denaro e a verificare gli enti di beneficenza prima di donare denaro o beni. La governatrice Hochul incoraggia, inoltre, i newyorkesi a restare in guardia quando divulgano dati sensibili online in un momento di aumento delle minacce alla sicurezza informatica attraverso l'utilizzo delle raccomandazioni di sicurezza del Dipartimento delle imposte e delle finanze (Department of Taxation and Finance). Ciò segue la creazione, da parte della governatrice, del Centro operativo di sicurezza comune (Joint Security Operations Center, JSOC), che funziona come centro per gli sforzi informatici congiunti locali, statali e federali.

La governatrice Hochul ha dichiarato: "New York ospita la più grande popolazione ucraina degli Stati Uniti e i newyorkesi danno sempre una mano per prendersi cura di chi ne ha bisogno". "Tuttavia, dobbiamo rimanere cauti nei confronti di coloro che cercano di commettere frodi, approfittando della gentilezza altrui. Senza perdere la tua volontà di aiutare i nostri amici e familiari ucraini, ricordati che se qualcosa sembra sospetto, probabilmente lo è. Incoraggia i tuoi amici e la tua famiglia, specialmente i tuoi familiari anziani, a stare attenti quando sono online".

Ogni volta che accadono delle catastrofi, gli artisti della truffa sfruttano le emozioni delle persone che cercano di aiutare. L'invasione dell'Ucraina fornisce un'opportunità ai truffatori di creare falsi enti di beneficenza o di fingersi convincenti vittime di guerra. Altri

progettano siti web per imitare il sito ufficiale di un'associazione legittima per rubare i soldi e/o i dati personali degli ignari donatori.

Il Segretario di Stato Robert J. Rodriguez ha dichiarato: "I newyorkesi sono noti per essere solidali e generosi con chi ha bisogno. Mentre la guerra in Ucraina imperversa, i truffatori continueranno ad operare con stratagemmi emotivi e false sollecitazioni pubblicitarie nel tentativo di truffare i consumatori. Incoraggio i newyorkesi a proteggere le proprie buone intenzioni e a fare sempre una ricerca su un ente di beneficenza prima di donare per assicurarsi che i soldi guadagnati duramente vadano a coloro che hanno un disperato bisogno del nostro sostegno".

Il commissario ad interim per le tasse e le finanze Amanda Hiller ha dichiarato: "La crisi globale in Ucraina ha intensificato la preoccupazione per gli attacchi informatici, quindi dobbiamo essere tutti attenti per evitare che informazioni riservate cadano nelle mani sbagliate, attacchi denial-of-service e altre conseguenze negative".

L'AD dell' Ufficio dei servizi informatici (Office of Information Technology Services, ITS) Angelo 'Tony' Riddick ha dichiarato: "Innumerevoli newyorkesi con le migliori intenzioni hanno donato a enti di beneficenza a sostegno del popolo dell'Ucraina e stanno facendo la differenza. Sfortunatamente, questa generosità crea anche nuove opportunità da sfruttare per i criminali informatici. Per proteggerti e per assicurarti che la tua generosa donazione arrivi sempre nelle mani di coloro che hanno veramente bisogno di aiuto, ITS chiede ai newyorkesi di seguire queste buone pratiche e di rimanere vigili alla luce delle recenti minacce online e delle truffe informatiche".

Il commissario della Divisione della difesa nazionale e dei servizi di emergenza (Division of Homeland Security and Emergency Services) Jackie Bray ha dichiarato: "Ogni newyorkese ha un ruolo da svolgere quando si tratta di proteggere i propri dati personali e di proteggersi dalle minacce informatiche. Sappiamo che nei momenti di bisogno, i malintenzionati sono là fuori e cercano di approfittare di coloro che cercano di aiutare. Se stai cercando di sostenere il popolo ucraino attraverso donazioni online o digitali, stai attento e segui queste buone pratiche per assicurarti che le tue donazioni siano autentiche e che le tue informazioni rimangano al sicuro".

Il senatore statale Kevin Thomas ha dichiarato: "Il fatto che così tanti newyorkesi si siano attivati per aiutare il popolo ucraino la dice lunga sui nostri vicini. Sfortunatamente, ha anche creato una prima opportunità per i truffatori di sfruttare questa crisi per un guadagno personale. Esorto i newyorkesi a rimanere vigili e a prendere ulteriori precauzioni per assicurarsi che i loro generosi contributi siano destinati a cause legittime".

Il deputato Nily Rozic ha dichiarato, "I truffatori cercano sempre nuovi metodi per ingannarti, anche durante una crisi internazionale. In un momento in cui i newyorkesi si uniscono per sostenere l'Ucraina nel momento del bisogno, è fondamentale che i consumatori siano dotati delle competenze e delle conoscenze per assicurarsi che la

loro generosità non venga sfruttata. Sono grato alla governatrice Hochul per aver assicurato che i newyorkesi non vengano truffati per la loro generosità".

I truffatori spesso si mettono in contatto tramite i social media, e-mail non richieste, telefonate o messaggi di testo. Possono chiedere di inviare denaro attraverso una app di pagamento come Cash App, Venmo o Zelle, trasferire il denaro su un conto bancario offshore o inviare carte regalo prepagate. Molte truffe recenti includono richieste di donazioni in criptovaluta, come Bitcoin o Ethereum. Gli artisti della truffa sono creativi e continueranno a pensare a nuovi modi per frodare le persone, quindi i consumatori devono essere sempre vigili.

Per evitare che il denaro delle donazioni cada nelle mani sbagliate, la Divisione per la protezione dei consumatori dello Stato di New York raccomanda di prendere le seguenti precauzioni:

- **Verifica la richiesta.** I truffatori si spacciano molto spesso per amici, familiari o amanti sui social media e chiedono donazioni; è facile copiare la foto e le informazioni anagrafiche di qualcun altro e creare un falso account online. Se ricevi una richiesta non sollecitata di donazione online, anche se sembra provenire da qualcuno che conosci, connettiti direttamente con la persona attraverso un altro mezzo di comunicazione per verificare la richiesta. Non cliccare su nessun link e non compilare moduli prima di aver verificato la fonte. Se la richiesta proviene da qualcuno che hai conosciuto online solo di recente, molto probabilmente è una truffa e dovresti essere particolarmente prudente.
- **Ricerca l'ente di beneficenza**. Non fare affidamento solamente sul sito web di un ente di beneficenza. Cerca online prima di donare a qualsiasi ente di beneficenza usando il nome del gruppo più termini di ricerca come "recensione" e "truffa". La Commissione commerciale federale (Federal Trade Commission) raccomanda di controllare give.org, charitynavigator. org, charitywatch.org, o candid.org per consultare i risultati e le valutazioni delle organizzazioni di beneficenza. Puoi anche controllare tramite l'Agenzia delle entrate (the Internal Revenue Service, IRS) se un ente di beneficienza sia effettivamente registrato. Inoltre, prima di donare la Procura Generale (Office of the Attorney General) consiglia di controllare il Registro degli enti di beneficenza (Charities Registry) per i bilanci per assicurarsi che l'ente sia fiscalmente solido.
- **Resisti alle strategie di persuasione.** Anche se la situazione è urgente, i consumatori dovrebbero resistere alla persuasione e alla tentazione di donare immediatamente. I truffatori spesso ti fanno pressione per donare immediatamente, facendoti dimenticare i campanelli d'allarme nella loro storia. Diffida delle e-mail dirette da "vittime" e promotori che utilizzano storie strazianti, insistendo affinché tu doni immediatamente. Non dare soldi per telefono a televenditori non sollecitati; invece, chiedi al chiamante di inviare materiale scritto sull'ente di beneficenza e su dove donare, se lo desideri.
- **Mantieni privati i dati personali.** Non fornire mai il tuo numero di previdenza sociale, il numero della tua carta di credito o di debito o altri dati personali di

identificazione in seguito ad una richiesta di beneficenza non sollecitata. Se doni online, assicurati che la tua connessione internet sia sicura prima di procedere con le richieste di donazione.

- **Chiedi come verranno spesi i tuoi soldi.** I consumatori vogliono sapere che i loro soldi vanno direttamente alle vittime. Un vero ente di beneficenza dovrebbe essere in grado di farti sapere quanto della tua donazione andrà direttamente al programma rispetto alle spese amministrative.

- **Dona con assegno o carta di credito.** Non donare mai soldi usando contanti, carte regalo, criptovalute o qualsiasi altra forma di denaro che sarebbe difficile da rintracciare. Dona il tuo contributo tramite assegno o carta di credito per assicurarti di avere una traccia della donazione. Intesta gli assegni all'ente di beneficenza, non ad un individuo. Se scegli di donare attraverso il sito web di un ente di beneficenza, controlla che il sito sia sicuro e che il tuo computer sia dotato dell'ultima protezione anti-virus.

Se sospetti di esserti imbattuto in un tentativo illegale di ricevere donazioni, puoi presentare un reclamo alla Divisione per la protezione dei consumatori dello Stato di New York a https://dos.ny.gov/file-consumer-complaint.

La linea diretta di assistenza ai consumatori della Divisione è aperta dal lunedì al venerdì, esclusi i giorni festivi, dalle 8:30 alle 16:30 al numero 1-800-697-1220. Puoi trovare ulteriori informazioni e consigli seguendo la Divisione di protezione dei consumatori sui social media su Twitter (@NYSConsumer) e Facebook (www.facebook.com/nysconsumer).

In mezzo alla crescente preoccupazione internazionale sulla sicurezza informatica, il Dipartimento delle imposte e delle finanze dello Stato di New York condivide anche una serie di consigli critici per aiutare i contribuenti a salvaguardare i loro dati personali durante la stagione fiscale e durante tutto l'anno:

Diffida delle email non richieste e delle telefonate in cui ti vengono richiesti dati personali. Non condividere mai dati personali, come il tuo numero di previdenza sociale, in risposta a un'e-mail o a una telefonata non richiesta. Se l'email o la telefonata afferma di provenire da un'azienda con la quale sei in affari, chiamala direttamente per confermare che il contatto sia legittimo. I truffatori spesso usano tattiche intimidatorie e minacce relative al debito tributario per farti condividere i tuoi dati personali e finanziari.

Mantieni al sicuro i tuoi dispositivi mobili. Esegui gli aggiornamenti del software che correggono le vulnerabilità conosciute non appena sono disponibili. Usa le opzioni di sicurezza incorporate nel tuo dispositivo, come un codice di accesso, e usa programmi che criptano i dati ed eliminano da remoto i contenuti se il dispositivo viene perso o rubato.

Fai attenzione agli hotspot Wi-Fi. Gli hotspot wireless pubblici non sono sicuri, il che significa che è facile per i ladri informatici vedere cosa stai facendo sul tuo dispositivo mobile mentre sei connesso. Limita quello che fai sul Wi-Fi pubblico ed evita di accedere ad account sensibili.

Conosci le tue app. Esamina accuratamente i dettagli e le specifiche di un'applicazione prima di scaricarla. Esamina e comprendi l'informativa sulla privacy di ogni app mobile. Sii consapevole che l'app potrebbe richiedere l'accesso alla tua posizione e ai tuoi dati personali.

Fai attenzione alle informazioni che condividi sui social media. Evita di pubblicare la tua data di nascita, numero di telefono, indirizzo di casa o immagini che identificano il tuo lavoro o i tuoi hobby. Per una ragione: questo tipo di informazioni può essere usato per determinare le risposte alle domande di sicurezza usate per resettare le password e ti trasforma in un obiettivo dei truffatori che cercano di accedere ai tuoi account e alle tue informazioni personali.

Usa password forti. Crea password diverse per tutti i tuoi account. Quando si tratta di password, cerca di usarne una con almeno 14 caratteri, lo standard attuale del settore. Usa una combinazione di lettere (maiuscole e minuscole), numeri e simboli. Considera le frasi d'accesso in cui usi le prime lettere di una frase memorabile per creare una password complessa e difficile da indovinare. Cambia regolarmente le password/frasi d'accesso.

Cambia le tue domande di sicurezza. Non utilizzare le stesse domande di sicurezza su più account. Seleziona domande di sicurezza per le quali le risposte non possono essere indovinate o trovate cercando sui social media o su internet.

Usa la verifica in due fasi per accedere ad un conto. Per aumentare la sicurezza degli account online, quando è possibile richiedere una password e un codice di sicurezza extra per verificare la tua identità quando accedi.

Attenzione al phishing. Non cliccare su link, scaricare file o aprire allegati in email da mittenti sconosciuti. Apri gli allegati solo quando li aspetti e sai cosa contengono, anche se conosci il mittente.

È importante rivedere regolarmente i passi necessari per proteggere i tuoi dati sensibili.

Denuncia. Se sei una vittima o credi di poter essere vittima di un furto d'identità relativo alle tasse, avvisaci immediatamente. Rintracceremo i tuoi dati per aiutarti a mantenerli privati e protetti. Visita la pagina web denuncia una frode, truffa o furto di identità del Dipartimento delle imposte.

Il Dipartimento delle imposte utilizza crittografia avanzata, firewall, sistemi di rilevamento delle intrusioni e altre misure di sicurezza per salvaguardare i nostri sistemi

e i dati sensibili, ma anche i contribuenti devono adottare un approccio proattivo per proteggersi online.

###