Do natychmiastowej publikacji: 22.03.2022 **GUBERNATOR KATHY HOCHUL**

GUBERNATOR HOCHUL OSTRZEGA KONSUMENTÓW PRZED OSZUSTWAMI I ZAGROŻENIAMI ZWIĄZANYMI Z CYBERBEZPIECZEŃSTWEM W ZWIĄZKU Z ROSYJSKĄ INWAZJĄ NA UKRAINĘ

Przekazuj darowizny sprawdzonym i renomowanym organizacjom, które wykorzystują je do niesienia pomocy potrzebującym Ukraińcom

Agencje stanowe wydają zalecenia dotyczące ochrony i zabezpieczania wrażliwych informacji oraz zachowania czujności w warunkach zwiększonego zagrożenia cyberbezpieczeństwa

Gubernator Kathy Hochul ostrzegła dziś mieszkańców stanu Nowy Jork przed oszustwami na tle akcji charytatywnymi i zwiększonym zagrożeniem cyberbezpieczeństwa w związku z inwazją Władimira Putina na Ukrainę. Wydział Ochrony Konsumentów Stanu Nowy Jork (New York State Division of Consumer Protection, DCP) dowiedział się o fałszywych prośbach o przekazanie pieniędzy na cele charytatywne, aby wesprzeć ofiary wojny. Zachęcamy konsumentów do uważnej oceny każdej prośby o pieniądze i sprawdzenia organizacji charytatywnych przed przekazaniem pieniędzy lub artykułów. Gubernator Hochul zachęca również mieszkańców stanu Nowy Jork do zachowania ostrożności przy udostępnianiu poufnych informacji w Internecie w obliczu wzrostu zagrożeń cyberbezpieczeństwa, wykorzystując zalecenia Departamentu Podatków i Finansów (Department of Taxation and Finance) dotyczące bezpieczeństwa. Jest to następstwem utworzenia przez gubernator Wspólnego Centrum Operacji Bezpieczeństwa (Joint Security Operations Center, JSOC), które pełni rolę centralnego ośrodka łączącego lokalne, stanowe i federalne działania w zakresie cyberbezpieczeństwa.

„Stan Nowy Jork jest domem dla największej populacji ukraińskiej w Stanach Zjednoczonych, a mieszkańcy stanu Nowy Jork zawsze wyciągają pomocną dłoń, by zadbać o tych, którzy są w potrzebie”, **powiedziała gubernator Hochul**. „Musimy jednak zachować ostrożność wobec tych, którzy próbują popełniać oszustwa, wykorzystując życzliwość innych. Pomagając naszym ukraińskim przyjaciołom i rodzinom, pamiętajcie, że jeśli coś wydaje się podejrzane, to prawdopodobnie takie jest. Zachęcajcie swoich przyjaciół i rodzinę, zwłaszcza bliskie osoby w starszym wieku, do zachowania czujności w sieci”.

Zawsze, gdy dochodzi do katastrofy, oszuści wykorzystują dobre sercach osób, które chcą pomóc. Inwazja na Ukrainę stanowi okazję dla oszustów do zakładania fałszywych organizacji charytatywnych lub podawania się za przekonujące ofiary wojny. Inni projektują strony internetowe imitujące oficjalne strony organizacji charytatywnych, aby wykraść pieniądze i/lub dane osobowe niczego niepodejrzewających darczyńców.

Sekretarz Stanu Robert J. Rodriguez powiedział: „Mieszkańcy stanu Nowy Jork znani są z tego, że wspierają i są hojni dla potrzebujących. Ponieważ wojna na Ukrainie trwa, nadal będą pojawiać się oszuści, którzy będą stosować emocjonalne sztuczki i fałszywe oferty, próbując oszukać konsumentów. Zachęcam mieszkańców stanu Nowy Jork, by dbali o swoje dobre intencje i zawsze sprawdzali organizacje charytatywne przed przekazaniem darowizny, aby mieć pewność, że ciężko zarobione dolary trafią do tych, którzy tak bardzo potrzebują wsparcia".

Pełniąca obowiązki Komisarz Departamentu Podatków i Finansów, Amanda Hiller, powiedziała: „Światowy kryzys na Ukrainie zwiększył obawy związane z cyberatakami, dlatego wszyscy musimy zachować czujność, aby zapobiec dostaniu się poufnych informacji w niepowołane ręce, atakom typu „odmowa usługi" (denial-of-service) i innym negatywnym skutkom".

Dyrektor ds. informacyjnych Biura Usług Informatycznych Stanu Nowy Jork (ITS), Angelo „Tony" Riddick, powiedział: „Niezliczona liczba mieszkańców stanu Nowy Jork w najlepszych intencjach przekazała datki na rzecz organizacji charytatywnych wspierających Ukraińców, a ich datki mają ogromne znaczenie. Niestety, ta hojność stwarza również nowe możliwości dla cyberprzestępców. Aby chronić siebie i mieć pewność, że hojna darowizna zawsze trafi do rąk tych, którzy naprawdę potrzebują pomocy, ITS prosi mieszkańców stanu Nowy Jork o przestrzeganie tych najlepszych praktyk i zachowanie czujności w świetle ostatnich zagrożeń internetowych i cyberoszustw".

Komisarz Stanowego Wydziału Bezpieczeństwa Wewnętrznego i Służb Ratowniczych, Jackie Bray, powiedziała: „Każdy mieszkaniec stanu Nowy Jork ma do odegrania ważną rolę, jeśli chodzi o zabezpieczenie swoich danych osobowych i ochronę przed zagrożeniami cyberbezpieczeństwa. Wiemy, że w czasach, gdy ludzie są w potrzebie, zdarzają się oszuści, którzy chcą wykorzystać tych, którzy próbują pomóc. Jeśli próbujesz wesprzeć obywateli Ukrainy poprzez darowizny internetowe lub cyfrowe, zachowaj czujność i postępuj zgodnie z poniższymi najlepszymi praktykami, aby mieć pewność, że Twoje darowizny trafią do rzeczywiście potrzebujących, a Twoje dane będą bezpieczne".

Senator stanu, Kevin Thomas, powiedział: „To, że tak wielu mieszkańców stanu Nowy Jork podjęło działania na rzecz pomocy narodowi ukraińskiemu, świadczy o naszych sąsiadach. Niestety, stało się to również doskonałą okazją dla oszustów do wykorzystania tego kryzysu do osiągnięcia osobistych korzyści. Apeluję do mieszkańców stanu Nowy Jork o zachowanie czujności i podjęcie dodatkowych środków ostrożności, aby mieć pewność, że ich szczodre datki trafią na słuszne cele".

Członkini Zgromadzenia, Nily Rozic, powiedziała: „Oszuści cały czas próbują nowych metod, nawet w czasie międzynarodowego kryzysu. Ponieważ mieszkańcy stanu Nowy Jork jednoczą się, aby wesprzeć Ukrainę w potrzebie, ważne jest, aby konsumenci posiadali umiejętności i wiedzę, które pozwolą im uniknąć wykorzystania ich hojności. Jestem wdzięczny gubernator Hochul za zapewnienie, że szczodrzy mieszkańcy stanu Nowy Jork nie będą oszukiwani".

Oszuści często nawiązują kontakt za pośrednictwem mediów społecznościowych, niechcianych e-maili, telefonów lub wiadomości tekstowych. Mogą prosić o wysłanie pieniędzy za pośrednictwem aplikacji płatniczych, takich jak Cash App, Venmo lub Zelle, przelanie pieniędzy na zagraniczne konto bankowe lub wysłanie przedpłaconych kart podarunkowych. Wiele niedawnych oszustw zawiera prośby o datki w kryptowalutach, takich jak Bitcoin czy Ethereum. Oszuści są kreatywni i wciąż wymyślają nowe sposoby wyłudzania pieniędzy, dlatego konsumenci muszą być zawsze czujni.

Aby zapobiec dostaniu się pieniędzy z darowizn w niepowołane ręce, Wydział Ochrony Konsumentów Stanu Nowy Jork zaleca podjęcie następujących środków ostrożności:

- **Zweryfikuj prośbę.** Oszuści coraz częściej podają się w mediach społecznościowych za przyjaciół, rodzinę lub romantyczne sympatie i proszą o datki; łatwo jest skopiować czyjeś zdjęcie i informacje biograficzne oraz stworzyć fałszywe konto w Internecie. Jeśli otrzymasz w Internecie nieproszoną prośbę o przekazanie darowizny, nawet jeśli wydaje Ci się, że jest to ktoś znajomy, skontaktuj się z tą osobą bezpośrednio za pomocą innego łącza komunikacyjnego, aby zweryfikować jej prośbę. Nie należy klikać na żadne linki ani wypełniać formularzy przed sprawdzeniem źródła. Jeśli prośba pochodzi od osoby, którą dopiero niedawno poznałeś(-aś) w Internecie, najprawdopodobniej jest to oszustwo i musisz zachować szczególną ostrożność.
- **Sprawdź informacje na temat organizacji charytatywnej**. Nie należy polegać wyłącznie na stronie internetowej organizacji charytatywnej. Przed przekazaniem darowizny na rzecz jakiejkolwiek organizacji charytatywnej poszukaj informacji w Internecie, używając nazwy grupy oraz haseł takich jak „recenzja" czy „oszustwo". Federalna Komisja Handlu (Federal Trade Commission, FTC) zaleca, aby sprawdzić następujące strony: give.org, charitynavigator.org,charitywatch.org lub candid.org, aby zapoznać się z raportami i ocenami organizacji charytatywnych. Można również skontaktować się z Urzędem Skarbowym(Internal Revenue Service, IRS), aby sprawdzić, czy dana organizacja charytatywna jest zarejestrowana. Biuro Prokuratora Generalnego (Office of the Attorney General) zaleca również sprawdzenie Rejestru Organizacji Charytatywnych (Charities Registry) w celu zweryfikowania sprawozdań finansowych przed dokonaniem darowizny, aby upewnić się, że dana organizacja charytatywna jest w dobrej kondycji finansowej.

- **Nie ulegaj presji.** Choć sytuacja jest pilna, konsumenci nie powinni ulegać naciskom, by natychmiast przekazać datki. Oszuści często naciskają na natychmiastowe przekazanie darowizny, przez co ofiarodawcy mogą przeoczyć pojawiające się sygnały ostrzegawcze. Należy uważać na bezpośrednie e-maile od „ofiar" oraz nagabujących, którzy opowiadają chwytające za serce historie, nalegając na natychmiastowe przekazanie darowizny. Nie należy przekazywać pieniędzy przez telefon telemarketerom. Zamiast tego należy poprosić rozmówcę o przesłanie pisemnych materiałów dotyczących organizacji charytatywnej i rachunku, na który można dokonać wpłaty.
- **Nie ujawniaj danych osobowych.** Nigdy nie podawaj numeru ubezpieczenia społecznego (Social Security), numeru karty kredytowej lub debetowej ani innych danych osobowych w odpowiedzi na prośbę o pomoc charytatywną pochodzącą od nieznanej osoby. Jeśli wpłacasz datki przez Internet, sprawdź, czy połączenie internetowe jest bezpieczne, zanim przystąpisz do realizacji darowizny.
- **Zapytaj, jak zostaną wydane Twoje pieniądze.** Konsumenci chcą wiedzieć, że ich pieniądze trafiają bezpośrednio do poszkodowanych. Prawdziwa organizacja charytatywna powinna być w stanie poinformować Cię, jaka część Twojej darowizny zostanie przeznaczona bezpośrednio na program, a jaka na opłaty administracyjne.

- **Przekaż darowiznę czekiem lub kartą kredytową.** Nigdy nie przekazuj gotówki, kart podarunkowych, kryptowalut ani innych środków płatniczych, które są trudne do wyśledzenia. Przekaż swój datek czekiem lub kartą kredytową, aby mieć pewność, że darowizna zostanie zarejestrowana. Czeki należy wystawiać na organizację charytatywną, a nie na osobę prywatną. Jeśli zdecydujesz się przekazać darowiznę za pośrednictwem strony internetowej organizacji charytatywnej, sprawdź, czy strona jest bezpieczna, a Twój komputer wyposażony w najnowszy program antywirusowy.

Jeśli podejrzewasz, że dotarła do Ciebie nieuczciwa próba otrzymania darowizny, możesz złożyć skargę do Wydziału Ochrony Konsumentów Stanu Nowy Jork pod adresem https://dos.ny.gov/file-consumer-complaint.

Infolinia Wydziału ds. pomocy konsumentom jest czynna od poniedziałku do piątku, z wyjątkiem świąt państwowych, w godzinach 8:30-16:30, pod numerem telefonu 1-800-697-1220. Więcej informacji i wskazówek można znaleźć, śledząc działalność Wydziału Ochrony Konsumentów w mediach społecznościowych na Twitterze (@NYSConsumer) oraz na Facebooku (www.facebook.com/nysconsumer).

W obliczu rosnącego międzynarodowego zaniepokojenia kwestią cyberbezpieczeństwa Departament Podatków i Finansów Stanu Nowy Jork przedstawia szereg istotnych wskazówek, które pomogą podatnikom chronić ich prywatne informacje w sezonie podatkowym i w ciągu całego roku:

Zachowaj ostrożność w przypadku niechcianych wiadomości e-mail i telefonów z prośbą o podanie danych osobowych. Nigdy nie udostępniaj danych osobowych, takich jak numer ubezpieczenia społecznego, w odpowiedzi na obcą wiadomość e-mail lub telefon. Jeśli wiadomość e-mail lub telefon pochodzi od firmy, z którą prowadzisz interesy, zadzwoń bezpośrednio do niej, aby potwierdzić wiarygodność prośby. Oszuści często stosują taktykę zastraszania i gróźb związanych z długami podatkowymi, aby nakłonić Cię do udostępnienia swoich danych osobowych i finansowych.

Zabezpiecz swoje urządzenia mobilne. Instaluj aktualizacje oprogramowania usuwające znane luki w zabezpieczeniach, gdy tylko staną się dostępne. Korzystaj z zabezpieczeń wbudowanych w urządzenie, takich jak kod dostępu, oraz używaj programów, które szyfrują dane i zdalnie usuwają zawartość w przypadku zgubienia lub kradzieży urządzenia.

Uważaj na hotspoty Wi-Fi. Publiczne hotspoty bezprzewodowe nie są bezpieczne, co oznacza, że cyberzłodzieje mogą łatwo sprawdzić, co robisz na swoim urządzeniu mobilnym, gdy jesteś podłączony do takiej sieci. Ogranicz czynności wykonywane w publicznych sieciach Wi-Fi i unikaj logowania się na wrażliwe konta.

Sprawdź swoje aplikacje. Przed pobraniem aplikacji należy dokładnie zapoznać się z jej szczegółami i specyfikacjami. Zapoznaj się z polityką prywatności każdej aplikacji mobilnej i zrozum ją. Należy pamiętać, że aplikacja może zażądać dostępu do informacji o lokalizacji i danych osobowych użytkownika.

Zachowaj ostrożność, jeśli chodzi o informacje, które udostępniasz w mediach społecznościowych. Unikaj zamieszczania daty urodzenia, numeru telefonu, adresu zamieszkania oraz zdjęć przedstawiających Twoją pracę lub zainteresowania. Jeden z powodów: tego typu informacje mogą być wykorzystywane do ustalania odpowiedzi na pytania zabezpieczające używane do resetowania haseł i sprawiają, że stajesz się celem oszustów, którzy próbują uzyskać dostęp do Twoich kont i danych osobowych.

Używaj silnych haseł. Utwórz różne hasła dla wszystkich swoich kont. Jeśli chodzi o hasła, staraj się używać takich, które mają co najmniej 14 znaków, co jest obecnie standardem branżowym. Należy używać kombinacji liter (dużych i małych), cyfr i symboli. Rozważ wprowadzenie haseł, w których wykorzystuje się pierwsze litery łatwego do zapamiętania wyrażenia w celu utworzenia złożonego i trudnego do odgadnięcia hasła. Regularnie zmieniaj swoje hasła dostępu.

Zmieniaj swoje pytania bezpieczeństwa. Nie używaj tych samych pytań zabezpieczających na wielu kontach. Wybierz pytania dotyczące bezpieczeństwa, na które odpowiedzi nie można odgadnąć ani znaleźć w mediach społecznościowych lub Internecie.

Korzystaj z dwustopniowej weryfikacji przy uzyskiwaniu dostępu do kont. Aby zwiększyć bezpieczeństwo kont internetowych, zawsze, gdy to możliwe, wymagaj

podania hasła i dodatkowego kodu zabezpieczającego w celu weryfikacji tożsamości użytkownika podczas logowania.

Uważaj na phishing. Nie klikaj linków, nie pobieraj plików ani nie otwieraj załączników w wiadomościach e-mail od nieznanych nadawców. Nawet jeśli znasz nadawcę, otwieraj załączniki tylko wtedy, gdy się ich spodziewasz i wiesz, co zawierają.

Ważne jest, aby regularnie sprawdzać, jakie kroki należy podjąć w celu zabezpieczenia poufnych informacji.

Zgłoś nadużycie. Jeśli padłeś(-aś) ofiarą lub podejrzewasz, że możesz paść ofiarą kradzieży tożsamości związanej z podatkami, natychmiast nas powiadom. Będziemy śledzić Twoje informacje, aby zachować ich prywatność i ochronę. Odwiedź stronę internetową Departamentu Podatków i wejdź w zakładkę Report fraud, scams, and identity theft (Zgłoś oszustwo, wyłudzenie i kradzież tożsamości).

Departament Podatków stosuje zaawansowane szyfrowanie, zapory sieciowe, systemy wykrywania włamań i inne środki bezpieczeństwa, aby chronić nasze systemy i poufne dane, ale podatnicy muszą również przyjąć proaktywne podejście do ochrony swoich danych w Internecie.

###