Per la diffusione immediata: 17/02/2017 **IL GOVERNATORE ANDREW M. CUOMO**

IL GOVERNATORE CUOMO AVVERTE IN MERITO ALLA NUOVA ONDATA DI CONTINUE TRUFFE SULLA TASSAZIONE CHE PRENDE DI MIRA CONSULENTI FISCALI E PROFESSIONISTI DEL SETTORE DELLE RISORSE UMANE

Almeno 37 compagnie con dipendenti di New York hanno subito furti d'identità che hanno compromesso oltre 5.000 numeri della previdenza sociale

Il Governatore Andrew M. Cuomo ha avvisato oggi i consulenti fiscali di New York e i professionisti delle risorse umane in merito a nuove truffe che hanno l'intento di appropriarsi di informazioni confidenziali di clienti e dipendenti, questo dopo che il Dipartimento delle imposte dello Stato di New York (New York State Tax Department) ha identificato almeno 37 aziende colpite nella Città di New York, Regione della capitale, New York centrale e New York occidentale, coinvolgendo migliaia di contribuenti.

"Dato che la tecnologia continua a progredire, truffatori e ladri cibernetici stanno utilizzando metodi sempre più sofisticati per appropriarsi di informazioni personali in modo da frodare i lavoratori di New York," **ha commentato il Governatore Cuomo.** "Utilizziamo una tolleranza zero in merito a queste truffe e incoraggiamo chiunque, specialmente coloro che appartengono a questi campi, a restare vigili e denunciare immediatamente alle autorità locali o statali qualsiasi richiesta sospetta."

Nonie Manion, attuale Commissario del Dipartimento delle imposte e delle finanze dello Stato di New York (New York State Department of Taxation and Finance) ha commentato, "Ora che sta per giungere il momento della compilazione delle tasse relative al reddito, i criminali sono pronti a contraffarle richieste per rimborsi relativi alle tasse utilizzando informazioni personali rubate. È fondamentale che chiunque gestisca informazioni personali sia consapevole delle comuni tecniche di frode, in modo da evitare di divenire una vittima."

Il Governatore Cuomo ha avvisato i newyorkesi in merito a svariate truffe sorte durante questo periodo di tassazione, includendo le seguenti:

Il rinnovato schema dei truffatori prende di mira i professionisti delle risorse umane e del settore della contabilità
I criminali telematici si fingono dirigenti di aziende inviando e-mail ai professionisti delle risorse umane e del settore della contabilità, in modo da richiedere elenchi di dipendenti e le loro rispettive informazioni personali. In questo momento, i truffatori stanno espandendo la loro area ad altri settori, includendo distretti scolastici, organizzazioni tribali e associazioni non profit.

Queste e-mail possono apparire legittime, dato che contengono il nome dell'amministratore delegato dell'azienda. In ogni caso, se ricevete una e-mail di questo tipo, nella risposta non includete mai alcun dettaglio relativo alla contabilità, come per esempio i formulari W-2 e i numeri della previdenza sociale.

Il Dipartimento delle imposte è consapevole di almeno 37 attività con dipendenti di New York che sono state vittime di questa tipologia di truffa e si stima che oltre 5.000 numeri della previdenza sociale siano stati compromessi. Il Dipartimento delle imposte è in contatto con queste aziende e sta lavorando con loro per proteggere i rispettivi dipendenti.

Se siete datori di lavoro vittime di questa truffa e avete risposto allegando dati relativi alla contabilità, come le informazioni W-2 e i numeri della previdenza sociale, seguite le istruzioni presenti sulla Guida per datori di lavoro truffati attraverso la frode W-2 phishing.

Schema Spear-Phishing che prende di mira i professionisti
Questo schema si è presentato all'interno della comunità dei professionisti nel campo fiscale. Viene utilizzato da truffatori che si presentano come appartenenti a Fastsupport.com o Onlyforsupport.com. Successivamente contattano i professionisti dopo aver identificato quale fornitore e-file autorizzato IRS, o Electronic Return Originator (ERO), è utilizzato dal professionista per trasmettere le informazioni.

Il richiedente, dichiarando falsamente di lavorare per ERO, suggerisce la necessità di reinstallare o correggere dei problemi attraverso il software del professionista. Il richiedente domanda al professionista di connettersi al proprio sito Web e fornire il codice segreto per poter così accedere al computer del professionista. Nel caso il professionista esegua tale richiesta, l'artista della truffa può rubare informazioni sensibili del cliente con l'intento di commettere una frode.

La sigla ERO identifica un fornitore e-file autorizzato IRS per inviare fascicoli relativi alla tassazione in modo che questi vengano elaborati.

I criminali telematici si fingono clienti per sollecitare servizi da professionisti del ramo fiscale
All'interno di uno schema di phishing a livello nazionale, i truffatori stanno prendendo di mira i professionisti del ramo fiscale per ottenere le loro informazioni relative alla contabilità e preparare così dei fascicoli fraudolenti. Questi truffatori inviano tipicamente due e-mail ai professionisti del ramo fiscale: all'interno della prima, un "cliente" richiede assistenza per la preparazione dei moduli relativi alla tassazione; all'interno della seconda, i truffatori forniscono un link, o un allegato PDF, che contiene un link che permette loro di rubare l'indirizzo e-mail e la password del commercialista.

Nel caso riceviate una e-mail sospetta, come per esempio una e-mail proveniente da un mittente sconosciuto, non selezionate alcun link né tanto meno aprite alcun allegato contenuto all'interno della e-mail. Si tratta di un truffatore che desidera accedere al vostro computer, esponendovi ad un malware. Questo può permettere al criminale telematico di ottenere informazioni sensibili senza che voi siate assolutamente consapevoli che ciò stia succedendo.

E-mail di phishing che utilizza come soggetto “Mails on Hold!” e prende di mira i professionisti del ramo fiscale
Alcuni professionisti del ramo fiscale hanno ricevuto e-mail che sembrano essere state inviate dall’IRS, o dal team di IRS e-Services, e nello spazio del soggetto viene scritto “Mails on Hold!” Queste e-mail potrebbero includere dei riferimenti a personale IRS o PTIN, ma non provengono dall’IRS.

Nel caso riceviate una e-mail con questo soggetto, non selezionate alcun link né tanto meno alcun allegato contenuto all’interno di queste e-mail. Farlo potrebbe garantire l’accesso al vostro computer, esponendoli a malware e rendendo vulnerabili le informazioni private.

Proteggete voi stessi e i vostri clienti
I professionisti del ramo fiscale devono proteggere le informazioni personali dei propri clienti fornendole solamente a fonti fidate come IRS e il Dipartimento delle imposte dello Stato di New York. Questo include fare a brandelli i documenti contenenti dati privati prima di eliminarli, ed inviare rapidamente i moduli relativi alla tassazione del cliente in modo da ridurre la tempistica durante la quale un ladro d'identità avrebbe l’opportunità di richiedere un rimborso fiscale fraudolento utilizzando tali informazioni.

Il Dipartimento delle imposte dello Stato di New York e l’IRS non effettueranno mai minacce via telefono e non richiederanno mai informazioni personali o finanziarie tramite e-mail.

Denuncialo
Se siete stati contattati da un truffatore che impersonava un agente IRS, dovete contattare immediatamente l’IRS. Scoprite qui come denunciare un incidente.

Se siete stati contattati da un artista della truffa che fingeva di appartenere al Dipartimento delle imposte dello Stato di New York, visitate la pagina Web denuncia una frode, truffa o furto di identità del Dipartimento delle imposte, in modo da scoprire come riportarlo. Il Dipartimento delle imposte revisionerà rapidamente ogni richiesta e implementerà l’azione necessaria quando appropriato.

###