



**Per la diffusione immediata: 11/24/2015 IL GOVERNATORE ANDREW M. CUOMO**

### **IL GOVERNATORE CUOMO METTE IN GUARDIA I NEWYORKESI PERCHÈ ESERCITINO LA MASSIMA ATTENZIONE ALLE TRUFFE DURANTE LA STAGIONE DEGLI ACQUISTI PER LE FESTIVITÀ**

Il Governatore Andrew M. Cuomo ha esortato oggi i newyorkesi perché si tutelino dal furto di identità e prestino attenzione alle truffe, durante i giorni di sconto del Black Friday, del Cyber Monday e per tutto il periodo degli acquisti natalizi.

“Questo periodo, caratterizzato dal desiderio di donare, purtroppo è considerato da ladri informatici e truffatori una straordinaria opportunità per sfruttare acquirenti privi di sospetti” **ha ricordato il Governatore Cuomo.** “Invito tutti i newyorkesi a non abbassare mai la guardia e prestare la massima attenzione durante gli acquisti natalizi, per evitare di restare vittima di queste pratiche senza scrupoli”.

Il Black Friday e il Cyber Monday segnano l’avvio ufficiale della stagione degli acquisti natalizi. Anche se questi giorni hanno lo scopo di fornire opportunità di affari da prendere al volo, sono anche alta stagione per i truffatori. Gli imbroglioni sfruttano la stagione degli acquisti natalizi per truffare i consumatori e rubare loro denaro e identità.

**Il Segretario di Stato di New York, Cesar A. Perales, ha puntualizzato:** “Il furto di identità e altri tipi di truffa senza scrupoli avvengono più frequentemente in questo periodo dell’anno. I suggerimenti e le indicazioni seguenti saranno utili per determinare nei newyorkesi meno stress e più piacere in queste festività. Vogliamo che i newyorkesi siano consapevoli dei loro diritti di consumatori, proponendo loro consigli preziosi che consentiranno di assumere precauzioni contro i truffatori, i quali considereranno il periodo festivo come un’occasione per strappare con l’inganno il denaro guadagnato con fatica”.

**Margaret Miller, Direttore informatico dello Stato di New York, ha avvertito:** “Le tecnologie odierne rendono eccezionalmente comodo acquistare on line: basta un clic del mouse o una strisciata sullo schermo. Benché rendano molto più semplici le transazioni per il consumatore, rendono anche più facile compiere crimini informatici per un hacker. Quando sono on line durante questo periodo festivo, i newyorkesi devono esercitare molta prudenza e avvalersi di questi suggerimenti per tutelarsi meglio”.

**Ted Potrikus, Presidente e Amministratore delegato di Retail Council of New York State, ha affermato:** “I commercianti di New York di ogni dimensione sono pronti a mettersi al servizio degli acquirenti, dalle vie dello shopping ai centri commerciali e fino ai loro siti Web, con ottimi prodotti, prezzi e assistenza. Occorre verificare che gli acquisti avvengano con commercianti di fiducia, conservare le ricevute per eventuali resi e, comunque, non esitare a rivolgersi ai dipendenti del negozio per qualsiasi dubbio! Siamo impazienti di vedervi nei nostri fantastici negozi in ogni parte dello Stato di New York!”

Dai dati della Federal Trade Commission (Commissione federale sul commercio), in tutta la nazione i consumatori hanno segnalato oltre 1,7 miliardi di dollari di perdite per frodi e furto di identità nel 2014. Il Centro per i ricorsi relativi a crimini su Internet del Federal Bureau of Investigation ha ricevuto nel 2014 denunce da oltre 14.000 newyorkesi, che hanno segnalato perdite per oltre 47 milioni di dollari a causa della criminalità informatica. Nello Stato di New York, durante l'ultimo periodo natalizio da novembre 2014 a gennaio 2015, sono state presentate dai consumatori oltre 3.000 denunce di furti di identità. La linea diretta della Divisione per la tutela dei consumatori riceve inoltre centinaia di chiamate durante le festività, da parte di consumatori che chiedono aiuto per evitare di restare vittime di truffe.

Attraverso l'Unità di assistenza ai consumatori, la Divisione riceve reclami di consumatori, tenta di mediare ove opportuno e rinvia i reclami all'agenzia federale, statale o locale competente, autorizzata dalla legge a procedere in materia. Tra l'altro, l'Unità di assistenza ai consumatori si pone come mediatore e risolve reclami riguardanti il rimborso e il reso di prodotti, controversie su carte di credito e attenuazione degli effetti del furto di identità.

Per ottenere le massime probabilità di accaparrarsi grandi affari, riducendo al tempo stesso il rischio di truffe e furto di identità, i consumatori devono acquistare da rivenditori notoriamente affidabili e attuare comportamenti sicuri on line. L'Ufficio dei servizi di Information technology della Divisione per la tutela dei consumatori dello Stato di New York propone i seguenti suggerimenti.

#### **Effettuare ricerche accurate.**

- **Acquistare solo da commercianti e siti Web che si conoscono e di cui si ha fiducia.** Non aprire un sito facendo clic su un collegamento inviato in una e-mail, trovato sul blog di qualcuno o in una pubblicità. Il sito Web d'arrivo potrebbe semplicemente assomigliare a quello reale, mentre magari è un falso molto ben congegnato. Se si nutrono dubbi sulla legittimità o la sicurezza di un negozio o un sito Web, è meglio non assumersi rischi.
- **Prestare la massima attenzione in caso di annunci fuorvianti.** Essere certi di aver capito l'offerta e leggere le clausole scritte in caratteri piccoli. Non cedere ad affari a prezzi stracciati a meno di accertarsi della loro legittimità, contattando il commerciante e ponendo domande prima di effettuare l'acquisto.
- **Pensarci bene prima di fare clic su collegamenti presenti nelle e-mail o su pubblicità a comparsa.** Quando si ricevono offerte non richieste via e-mail o appaiono annunci che sembrano provenire da negozi legittimi, occorre essere

molto diffidenti rispetto alla loro provenienza. Accanto alla possibilità di virus, questi annunci potrebbero essere truffe capaci di rubare denaro o vendere prodotti taroccati.

- **Leggere le procedure del negozio in materia di rimborsi, date di consegna e spedizione/gestione.** Prima di effettuare qualsiasi acquisto, chiedere le politiche del negozio. Controllare il genere di condizioni in cui devono trovarsi le merci per riuscire a effettuare un reso e se il negozio impone una maggiorazione per il reintegro in magazzino.
- **Prestare la massima attenzione riguardo alle potenziali truffe circa le donazioni di beneficenza.** Pensarci bene prima di fare clic su e-mail che richiedono donazioni. Per donare, è preferibile visitare l'indirizzo ufficiale affidabile del sito dell'ente di beneficenza e non servirsi mai di un collegamento presente in una e-mail.

### **Proteggere le informazioni che rendono identificabile la propria persona.**

- **Mettere in sicurezza il proprio computer e i dispositivi mobili.** [Mantenere aggiornato il software antivirus e antispyware, oltre al firewall.](#) Essere prudenti riguardo ai download gratis: la gratuità può diventare molto costosa. I salvaschermo, i biglietti elettronici o altri download gratis per le festività possono contenere virus.
- **Non utilizzare il Wi-Fi pubblico per operazioni bancarie personali o acquisti on line.** Le informazioni personali non devono mai essere inviate attraverso connessioni wireless non sicure in luoghi pubblici.
- **Mettere in sicurezza il Wi-Fi domestico.** Tenere sempre sotto controllo chi dispone di diritti di amministrazione e il livello di sicurezza della password di chi utilizza la rete. Le impostazioni di codifica devono essere attive e molto difficili da intuire.
- **Mettere in sicurezza gli acquisti.** Verificare che l'indirizzo URL inizi con "https". La "s" finale significa "sicuro" e indica che le comunicazioni con la pagina Web sono codificate e, di conseguenza, i propri dati sono protetti.
- **Assumere precauzioni circa le password utilizzate negli account on line.** Utilizzare password diverse per account on line diversi, specialmente per quelli legati ai propri dati finanziari. Creare password lunghe e complesse, utilizzando sia lettere minuscole che maiuscole, caratteri speciali e numeri. In genere, si consiglia una password di almeno 10 caratteri. Esaminare l'ipotesi di modificare le password al termine del periodo degli acquisti natalizi. Dopo aver completato la transazione on line, verificare di aver effettuato la disconnessione dal sito Web.
- **Sfuggire le offerte non richieste.** Quando si acquista on line, digitare il nome del sito da visitare, piuttosto che fare clic su offerte presenti su email o caselle a comparsa, che potrebbero comportare il rischio di furto di identità e frodi.  
**Una e-mail che chiede dati personali o finanziari è con la massima probabilità una truffa.**
- **Non rispondere alle e-mail non richieste in cui si domanda la password, il PIN o altri dati sensibili via e-mail.** Un soggetto legittimo non avvierà mai i contatti tramite i social media o una e-mail con la richiesta di dati personali o

finanziari. Se la e-mail sembra provenire dalla propria banca o azienda emittente della carta di credito, contattare direttamente tali soggetti.

- **Pagare con una carta di credito.** Quando si acquista on line o in un negozio, utilizzare assolutamente una carta di credito, non una carta di debito. Le carte di credito rientrano nella legge Fair Credit Billing Act (Legge sulla fatturazione del credito equo), che offre una maggiore protezione contro addebiti fraudolenti e consente di contestare più facilmente un oggetto sulla fattura, se non viene ricevuto. Prendere in esame l'ipotesi di una carta di credito da dedicare esclusivamente agli acquisti on line, in modo che possa essere colpita una sola carta, qualora un commerciante o un elaboratore di carte di credito subisca una violazione. Se si paga in contanti, conservare le ricevute.

#### **Conservare la documentazione.**

- **Conservare la procedura in forma cartacea.** Conservare la documentazione delle transazioni on line, comprendente la descrizione del prodotto, il prezzo, le condizioni, le garanzie, la ricevuta on line e le e-mail inviate e ricevute intercorse con il commerciante.

- **Prestare la massima attenzione ai piccoli addebiti sugli estratti conto.** Gli hacker si servono di piccoli addebiti a fini di verifica. Qualsiasi addebito non noto potrebbe essere un indizio di compromissione della carta.

#### **Attivarsi se si ritiene di essere vittime di un crimine informatico.**

- **Contattare il vostro istituto finanziario.** Notificare immediatamente alla banca, all'azienda emittente della carta di credito e qualsiasi altro soggetto dove si possiedono account, per informarli che qualcuno sta utilizzando dolosamente il conto.

- **Reimpostare le password.** Dopo l'attacco di un hacker, è possibile che siano state rubate anche le password degli altri account. Reimpostare le password innanzitutto degli account critici, iniziando dall'account della posta elettronica, cui faranno seguito gli account finanziari e comunque critici. È importante iniziare dalla posta elettronica, poiché le reimpostazioni di password per tutti gli altri account vengono generalmente inviate tramite e-mail.

- **Congelare i conti di credito.** Contattare tutti e tre i più importanti uffici del credito (Experian, Equifax e TransUnion) per chiedere una relazione sul credito; inoltre chiedere che sul proprio conto siano applicati un avviso di frode e un congelamento del credito.

- **Rivolgersi alla stazione di polizia locale.** Presentare una segnalazione perché esista una documentazione ufficiale dell'episodio.

Per maggiori informazioni o per presentare un reclamo nei confronti di un'azienda, è possibile visitare la Divisione per la tutela dei consumatori del Dipartimento di Stato di New York, al suo sito Web <http://www.dos.ny.gov/consumerprotection/>, oppure contattare la linea diretta della Divisione stessa al numero (800) 697-1220. La linea diretta per l'assistenza ai consumatori (Consumer Assistance Hotline) segue il seguente orario: da lunedì a venerdì (escluse le feste federali) dalle 8:30 alle 16:30.

È possibile seguire la Divisione per la tutela dei consumatori sui social media su Twitter [@NYSConsumer](#) e [Facebook](#)

Per altri consigli e risorse relative alla sicurezza on line, compresi avvisi riguardanti rischi emergenti, consigli quotidiani e molti materiali per la prevenzione semplici da utilizzare, è possibile visitare on line l'Office of Information Technology Services (Ufficio dei servizi di Information technology) alla pagina <http://www.its.ny.gov/>

L'Office of Information Technology Services si può seguire su Twitter [@NYStateCIO](#) e [Facebook](#)

###

Ulteriori notizie sono disponibili sul sito [www.governor.ny.gov](http://www.governor.ny.gov)  
Stato di New York | Executive Chamber | [press.office@exec.ny.gov](mailto:press.office@exec.ny.gov) | 518.474.8418