Caro newyorkese,

La tua identità è a rischio. Sulla rete, al telefono e anche di persona, per i truffatori è più facile che mai rubare le tue informazioni personali e usarle per commettere frodi.

Il furto di identità colpisce milioni di persone ogni anno. I truffatori richiedono carte di credito a tuo nome, ricevono le tue prestazioni mediche e usano persino il tuo numero di social security per la frode fiscale, danneggiando il tuo credito e costando tempo e denaro per risolverlo.

Puoi salvaguardare le tue informazioni personali e prevenire la maggior parte delle forme di furto di identità con un po' di diligenza, e noi siamo qui per aiutarti a capire come fare.

Per maggiori dettagli su come proteggere la tua identità o cosa fare se ritieni che la tua identità sia stata rubata, visita il nostro sito Web ag.ny.gov.

Cordiali saluti,

Letitia James

Procuratore Generale
di New York
Letitia James

Risorse

Ufficio del Procuratore Generale dello Stato di New York, Ufficio per la Tutela dei Consumatori contro le Frodi

Per segnalare truffe o presentare un reclamo.

(800) 771-7755 / ag.ny.gov

Commissione Federale per il Commercio

Per segnalare truffe o furti di identità

877- 382-4357 / ftc.gov

Resoconto creditizio

Per controllare o congelare il tuo credito

877-322-8228 / annualcreditreport.com

Principali agenzie di resoconto creditizio

Experian:
(888) 397-3742 / experian.com

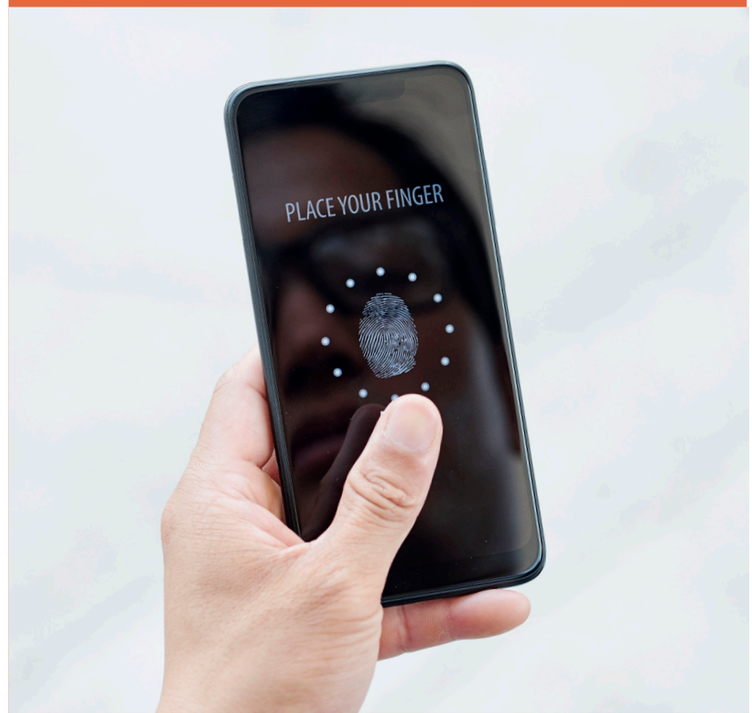
TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

Proteggi la tua identità

Suggerimenti per mantenere al sicuro la tua identità



Ufficio del Procuratore Generale
dello Stato di New York
Letitia James

Proteggi le tue informazioni personali

Sebbene sia generalmente sicuro fornire il tuo nome o numero di telefono, comunicare a qualcuno la tua data di nascita, il numero di social security o il numero di un qualsiasi conto può esporti al furto di identità. Dovresti anche evitare di divulgare le informazioni che utilizzi come risposta di "backup" che i siti web ti chiedono quando hai dimenticato una password.

Non fornire mai le tue informazioni personali a qualcuno che ti contatta a caso: a meno che sia tu ad averlo contattato, c'è la possibilità che tu venga "phished".

Il phishing è un tentativo di convincere una vittima a fornire informazioni personali quali nome utente, password o numero di carta di credito. I truffatori ti possono contattare tramite SMS, telefono o e-mail e spesso fingono di appartenere a un'agenzia governativa, a una banca o a una nota azienda. Richiederanno le tue informazioni personali al fine di risolvere un problema o un'emergenza, o diranno che devono solo "confermare le tue informazioni" prima che possano darti qualcosa.

Nessuna di queste organizzazioni ti contatterebbe in questo modo per informazioni importanti. Se non sei sicuro, chiama l'azienda, utilizzando i numeri pubblicati, per verificare se si tratta effettivamente di loro. In alcuni tentativi di phishing ti chiedono di accedere a un sito Web o di aprire un allegato. Non scaricare allegati o cliccare su links inviati dà persone che non conosci. Questi possono contenere virus che infetteranno il tuo computer e ruberanno le tue informazioni personali.

Messaggi sospetti

Anche se un messaggio sembra provenire da una fonte attendibile quale un parente o una nota azienda, potrebbe comunque trattarsi di un tentativo di phishing: i truffatori potrebbero aver preso il controllo dell'account o creato un nuovo account con un nome simile. Se ricevi un messaggio che non sembra inviato dal mittente, contiene solo un link o un allegato senza alcuna spiegazione o comunque sembra sospetto, controlla due volte il campo "da" per assicurarti che sia l'indirizzo corretto o chiama il mittente per verificare che sia davvero lui/lei. Questo può accadere sui social media come tramite e-mail o SMS; quindi, non fidarti di un messaggio sospetto solo perché proviene da un "amico".

Numero di Social Security

Non c'è bisogno che un'azienda richieda il tuo numero di previdenza sociale. Se lo fanno, chiedi perché ne hanno bisogno, soprattutto se non è un'agenzia governativa, un datore di lavoro, una banca o un istituto finanziario. E, ancora una volta, non darlo mai a qualcuno che ti contatta senza che sia richiesto.

Usa i Firewall, aggiorna il tuo sistema operativo

La navigazione sul Web può esporre il tuo computer a virus. Mantieni aggiornati il tuo sistema operativo e il tuo programma antivirus e mantieni il firewall in esecuzione per stare al sicuro

Crea password complesse

Se usi Internet, hai bisogno di password complesse e molte di esse. Una password complessa è quella che:

- È lunga. Dovrebbe includere almeno otto caratteri, ma più sono e meglio è.
- Non può essere indovinata da qualcuno che fa ricerche su di te, quindi niente compleanni o nomi di parenti.
- È qualcosa che puoi ricordare. Qui può essere utile usare una combinazione di parole lunghe e non comuni ("pinzatriceabatteria").
- La usi solo una volta. Se ripeti una password e qualcuno la apprende una volta, potrà accedere a tutti i tuoi account.

Gestori di Password

I browser moderni dispongono di "gestori di password" che puoi installare e che ricordano le tue password per te: basta scaricare un gestore e tutto il resto viene eseguito automaticamente. Mantieni la password del tuo gestore il più sicura possibile: se un truffatore riesce ad accedervi può accedere a tutti i tuoi account.

Dispositivi protetti della password

Tratta i telefoni cellulari e gli account dei computer proprio come gli account su un sito Web: assegna loro password uniche e sicure.

Password predefinite

Alcuni dispositivi, come il router o il modem, sono dotati di una password predefinita. Le password predefinite sono raramente sicure, quindi dovresti cambiarle immediatamente.

Cambia regolarmente le password

Anche se segui questi consigli, più a lungo usi una password, più è probabile che un malintenzionato riesca a ottenerla: i siti Web possono subire una violazione della sicurezza. Cambia sempre una password se il sito Web in questione viene violato e comunque cambia periodicamente le password per stare al sicuro.

Connessioni sicure

Un sito Web o una rete Wi-Fi non sicuri possono esporre le tue informazioni personali. Non condurre mai affari personali o finanziari su una rete pubblica e verifica che un sito Web sia "sicuro" prima di fornirgli informazioni riservate. I siti Web protetti inizieranno con **"https://"** anziché con **http://**

Elimina i dati non necessari

Distruggi tutti i record di informazioni personali una volta che non ne hai più bisogno. Distruggi documenti materiali quali ricevute, dichiarazioni dei redditi e cartelle cliniche o informazioni finanziarie; elimina o disattiva gli account digitali ed elimina i documenti digitali. Ricorda che anche se eliminati i documenti digitali possono essere ancora sul tuo disco rigido [hard drive]; quindi, se ti stai sbarazzando di un vecchio computer, avrai bisogno di un software di sicurezza speciale per cancellare tutti i tuoi dati personali.

Monitora gli estratti conto bancari

Controlla attentamente la carta di credito e gli estratti conto bancari per qualsiasi attività non autorizzata.

Controlla attentamente le fatture mediche e l'assicurazione sanitaria per assicurarti di aver effettivamente ricevuto il trattamento descritto.

Resoconti creditizi

Ogni anno ciascuno ha diritto a ricevere una copia gratuita del suo resoconto creditizio da ciascuna delle principali agenzie di segnalazione del credito. Se vedi accounts o richieste che non hai avviato o non riconosci, ciò potrebbe indicare che qualcun altro sta usando la tua identità. È possibile pianificare di ricevere rendiconti da diverse agenzie in diversi periodi dell'anno per ottenere una copertura regolare su annualcreditreport.com o (877) 322-8228

Furto di identità dei minori

Le identità dei minori sono quelle rubate più comunemente, a volte da membri della famiglia con rating creditizi scadenti. Proteggi le informazioni personali dei tuoi figli come faresti con le tue. Assicurati di porre domande e di agire se loro ricevono chiamate per la riscossione di fatture o offerte di credito a loro nome, se gli vengono negati dei sussidi perché qualcun altro sta utilizzando il loro numero o se ricevono avvisi dall'IRS riguardo a tasse non pagate.