# S.A.F.E.

## Senior Anti-Fraud Education

**S**enior = *Anziani*

**A**nti = *Anti*

**F**raud = *Frode*

**E**ducation = *Educazione*

Impara a riconoscere le truffe prima di rimanere vittima di una frode

NEW YORK STATE OF OPPORTUNITY.

**Division of Consumer Protection**

Tutelare e responsabilizzare i consumatori di New York

Divisione del Dipartimento di Stato di New York (New York Department of State)

Kathy Hochul, Governatore

Rossana Rosado, Segretario di Stato

# *Impara a riconoscere i rischi*

*Molto spesso sono i cittadini anziani a subire le truffe ai danni dei consumatori. I truffatori prendono di mira chi è più in là negli anni perché si tratta di soggetti considerati vulnerabili: una facile preda a cui sottrarre contanti. È importante conoscere nei dettagli queste attività per non rischiare di rimanerne vittima. Provvederemo dunque a illustrare sei delle truffe più frequenti a danno degli anziani, offrendo utili consigli per evitarle.*

* * * * *

## • Truffa dei dispositivi medici

Alcuni anziani segnalano di aver ricevuto messaggi preregistrati non richiesti, noti come “robocall”, che offrono gratuitamente dispositivi medici di segnalazione e buoni sconto per l’acquisto. Dopo aver risposto, una voce registrata chiede all’utente di premere il tasto 1 per ricevere gratuitamente un dispositivo, indicando l’indirizzo e i dati della carta di credito. Premendo 1, l’utente entra in contatto con un operatore, che cerca di sottrarre al malcapitato le sue informazioni personali e finanziarie. Inoltre, anche se il messaggio permette di selezionare un altro numero per rifiutare la chiamata, questa operazione comunica ai truffatori un numero telefonico attivo, che potrà essere utilizzato successivamente per effettuare altre chiamate a scopo di truffa.

## • Truffa del nonno

**Questi truffatori chiamano al telefono o inviano e-mail agli anziani per chiedere soldi, spacciandosi per parenti che hanno bisogno di un aiuto economico. Spesso le chiamate arrivano nel bel mezzo della notte, e la persona che risponde al telefono può essere disorientata. Gli impostori riescono a sembrare credibili grazie alla loro capacità di sfruttare informazioni personali trovate sui social media e su Internet. In alcune circostanze cercano di farsi passare per agenti delle forze dell'ordine, avvocati o medici che chiamano per conto di un finto parente che si è messo nei guai. In ogni caso, chiedono sempre l'invio immediato di denaro, di solito a mezzo bonifico.**

## • Truffa del ghosting

"Ghosting" se yon fòm vòl idantite. Vòlè idantite yo jwenn enfòmasyon pèsonèl sou moun ki mouri nan avi lanmò moun, ponp finèb, lopital, sètifika lanmò yo vòlè, ak sitwèb sou entènèt. Lè yo gen enfòmasyon yo, sitou nimewo Sekirite Sosyal, yo itilize enfòmasyon yo pou jwenn kredi epi pou louvri kont, pran lajan prete, resevwa avantaj, oswa menm touche ranbousman lajan taks avèk idantite yo vòlè a. Manm fanmi moun ki mouri yo pa responsab pou frè ki dwe peye akòz kalite vòl idantite sa a toutotan non yo pa sou kont yo vòlè a. Sonje, li enpòtan pou fè Administrasyon Sekirite Sosyal (Social Security Administration) konnen yon ka lanmò.

## • Truffa dell'incarico in giuria

Questi truffatori si fanno passare per agenti delle forze dell'ordine o funzionari del tribunale e contattano le vittime designate, informandole che non hanno risposto a una convocazione per far parte di una giuria e che dunque, per evitare l'arresto, devono pagare una multa con carta di credito. In molti casi, quando la vittima informa chi l'ha chiamata di non aver ricevuto alcuna convocazione, l'interlocutore ribatte che il cittadino è tenuto a presentarsi in tribunale anche se non ha ricevuto alcun avviso. Questi truffatori cercano di sottrarre alle vittime informazioni personali come il numero di previdenza sociale e la data di nascita, che potranno poi utilizzare per mettere in atto furti di identità o altre attività fraudolente.

## • Truffa dell'avviso funebre (Funeral Notification)

Queste truffe prevedono l'invio di e-mail con l'oggetto "funeral notification" a destinatari che vengono ingannevolmente informati di una cerimonia di commiato che sarà tenuta a breve in memoria di un amico o di un parente. Le mail, che sembrano a tutti gli effetti inviate da agenzie di pompe funebri, chiedono a chi le riceve di fare clic su un link per avere "maggiori informazioni". Il link reindirizza la vittima a un sito web in cui viene subito attivato il download di un malware, ovvero un software che si infiltra nel sistema operativo e consente ai truffatori di accedere a informazioni conservate nel computer, che verranno poi utilizzate per altre attività fraudolente. Se ricevi una mail come questa, cancellala immediatamente.

## • Truffa della lotteria

Purtroppo, molte lotterie vengono organizzate da truffatori con l'obiettivo di accedere a dati e conti personali. I truffatori prima adescano i malcapitati offrendo fantastici premi, e poi chiedono loro di indicare le informazioni personali o di versare un contributo per partecipare alla lotteria. Queste truffe prendono spesso di mira gli anziani, che versano il contributo e ricevono assegni falsi depositati sui loro conti bancari con cui vengono illusi di aver vinto effettivamente qualcosa. Gli assegni vengono però rifiutati, poiché risultano contraffatti. Nel frattempo, i truffatori hanno intascato i contributi e le imposte sui premi. Per partecipare a una lotteria legale non bisogna mai versare alcun contributo.

## • Truffa dell' IRS

Questa frode è un esempio di "phishing", ed è una delle truffe telefoniche più sofisticate mai realizzate: secondo una stima dell''Agenzia delle entrate (Internal Revenue Service, IRS), almeno 20.000 contribuenti ne sono stati vittime. Facendosi passare per funzionari dell'IRS, i truffatori chiedono alle vittime di versare immediatamente tasse arretrate effettuando un addebito con carta o bonifico, per evitare l'arresto. Dimostrano perfino di conoscere le ultime quattro cifre del numero di previdenza sociale delle vittime e, come segnalano le vittime, inviano anche una mail a seguito della conversazione telefonica. Se si riceve una chiamata inattesa

dall'IRS, è molto probabile che sia un tentativo di truffa. Tuttavia, non sempre è facile riconoscerlo come tale. Per farlo, bisogna tenere presente che l'IRS di solito invia un avviso postale prima di effettuare qualsiasi intervento e non chiede mai all'utente di corrispondere immediatamente l'importo dovuto. In caso di dubbi, si consiglia di interrompere la comunicazione e chiamare uno dei numeri dell'IRS disponibili sull'apposito sito web o nell'elenco telefonico: 1-800-829-1040.

## • Truffa dei finanziamenti gratuiti

**Bisogna fare sempre attenzione ai finanziamenti promessi per iscritto o al telefono. In un caso è perfino accaduto che alcuni finanziamenti siano stati pubblicizzati su giornali e riviste prima di rivelare la loro natura fraudolenta. L'annuncio affermava che i lettori erano idonei a ricevere finanziamenti gratuiti per sostenere diverse spese per interventi di ristrutturazione domestica, tasse universitarie, bollette arretrate e lavoro da remoto. In altri casi, le vittime hanno segnalato di aver ricevuto telefonate da persone che si spacciavano per rappresentanti di un'organizzazione o di un'agenzia governativa e che, snocciolando una serie di titoli e sigle altisonanti, promettevano di elargire finanziamenti gratuiti per aver pagato regolarmente le tasse o per estinguere alcuni debiti. Il metodo adottato da queste persone è sempre lo stesso: si congratulano con il loro interlocutore, per poi cercare di sottrargli informazioni personali e finanziarie. Confermano nome e recapito postale della vittima, dopodiché chiedono il nome della banca, il numero dei conti e i codici bancari, e la rassicurano dicendo che queste informazioni verranno utilizzate solo per ritirare l'importo di una tassa di gestione. Indipendentemente dal metodo scelto, le loro promesse non cambiano: la domanda verrà accettata automaticamente, e il finanziamento sarà a fondo perduto. Offrire finanziamenti può nascondere una truffa da parte di persone che vogliono avere accesso al conto corrente di qualcun altro.**

# Consigli per evitare le truffe

- Interrompi la conversazione telefonica senza premere alcun tasto, se ricevi una chiamata inattesa. Se rispondi alla telefonata, verifica sempre l'identità del chiamante e della società che rappresenta. Inoltre, procurati sempre un numero telefonico dell'azienda
- Non fornire mai informazioni personali o finanziarie al telefono, come ad esempio nome, data di nascita, numero di previdenza sociale, indirizzo e numero Medicare.
- Contatta il tuo gestore telefonico chiedendogli di bloccare i numeri "robocall". Non fare affidamento su altri servizi che bloccano le robocall, perché i numeri visualizzati cambiano frequentemente.
- Installa un firewall e un software antivirus o antispyware per proteggere il tuo account email, impedendo ai truffatori di accedervi. Inoltre, aggiorna sempre tutti i programmi del computer.
- Non aprire allegati inviati da persone che non conosci o mail che sembrano sospette. Gli allegati possono contenere programmi che permettono ai truffatori di accedere al computer della vittima.
- Non indicare mai data di nascita, cognome da nubile o altri dati identificativi personali di amici o familiari nei necrologi, poiché queste informazioni potrebbero essere utilizzate per compiere un furto di identità.
- Non aprire mai file allegati a mail sospette per non rischiare di scaricare inavvertitamente un software malevolo.
- Non rispondere a offerte di premi per una lotteria in cambio di un contributo.

- Il primo contatto con l'IRS per la riscossione di tasse arretrate avviene attraverso il servizio postale degli Stati Uniti e mai tramite e-mail o telefonicamente.
- L'IRS non chiede mai di pagare tramite bonifico o carta di debito prepagata.
- Contatta direttamente l'IRS al numero 800-829-1040, se pensi di essere in arretrato con il pagamento delle tasse.
- Tutela i tuoi dati personali archiviandoli in un luogo sicuro e protetto. Non conservare i numeri dei conti o altri dati sensibili nel portafoglio o nello smartphone.
- Ricorda sempre che le chiamate telefoniche possono essere ingannevoli. I truffatori possono adottare anche metodi sofisticati per modificare i prefissi nei sistemi di identificazione del chiamante.
- Non pagare per ricevere finanziamenti governativi "a titolo gratuito": se ti chiedono di effettuare un pagamento per ricevere un finanziamento governativo si tratta sicuramente di una frode.
- Non inviare mai fondi a mezzo bonifico e non pagare un prodotto/servizio tramite vaglia. Le aziende accettano sempre pagamenti con carta di credito o assegni circolari. Questo ti aiuterà a riconoscere il pericolo e a bloccare il pagamento.
- Non versare mai somme in contanti e non pagare mai completamente lavori di ristrutturazione domestica prima che siano stati portati a termine. In genere, le ditte chiedono solo una somma in anticipo per procedere con i lavori di ristrutturazione, senza pretendere di ricevere subito l'intero importo.

# S.A.F.E.

## Senior Anti-Fraud Education

Impara a riconoscere le truffe prima di rimanere vittima di una frode

### Se sei stato vittima di una truffa:

- Contatta la polizia locale o l'ufficio dello sceriffo per segnalare il reato.
- Informa i vicini di casa e le associazioni locali della presenza di truffatori nella vostra zona.
- Contatta la Divisione per la tutela dei consumatori (Divisione of Consumer Protection) all'indirizzo https://dos.ny.gov, il Procuratore generale (Attorney General's Office) all'indirizzo www.ag.ny.gov e/o l'agenzia locale per la tutela dei consumatori per richiedere assistenza e informare la comunità.
- Prendi nota delle perdite finanziarie che hai subito, in vista di un


NEW YORK STATE OF OPPORTUNITY.

Division of Consumer Protection

Tutelare e responsabilizzare i consumatori di New York

Divisione del Dipartimento di Stato di New York (New York Department of State)

1-800-697-1220 https://dos.ny.gov

@nysconsumer /nysconsumer


09/21-IT