

Proteggiti dalle truffe

Una truffa è un'attività disonesta o illegale che convince con l'inganno le persone a dare denaro, informazioni personali, immagini intime o qualcos'altro di valore. Una truffa online è generalmente gestita da qualcuno con un profilo falso o un'attività commerciale falsa. Quindi, anche se Internet può essere un posto meraviglioso da esplorare, vale la pena essere cauti!

Essere consapevole che esistono i truffatori è uno dei passi importanti per evitarli. Una volta che conosci i loro trucchi, è più probabile che tu sia in grado di individuare una truffa. Stare all'erta è la tua migliore difesa.

Ecco alcuni suggerimenti per riconoscere ed evitare le truffe.



Proteggi le tue informazioni personali

I truffatori cercano di accedere alle tue informazioni personali facendoti domande o dandoti istruzioni tramite una telefonata, per e-mail, SMS o tramite i social media. I truffatori useranno i tuoi dati personali per rubarti soldi o commettere un altro crimine.

Cosa chiedono i truffatori?

I truffatori cercano di ottenere la tua fiducia fingendo di appartenere a un'organizzazione o agenzia ben nota come NBN Co, Telstra, Microsoft, Australia Post, l'ufficio delle imposte, la polizia o Services Australia (MyGov, Centrelink, Medicare).

Per convincerti con l'inganno a rivelare le tue informazioni personali o finanziarie, i truffatori possono:

- Farti cliccare su un collegamento
- Chiederti di dare loro accesso remoto al tuo computer
- Chiederti di pagare un debito
- Chiederti di comprare un buono acquisto per pagare una multa
- Chiederti di trasferire fondi o inviare denaro all'estero.

Segni che potrebbe trattarsi di una truffa

Stai attento a:

- E-mail, messaggi o chiamate che sono inaspettati o vengono da qualcuno che non conosci
- Promesse di denaro
- Minacce di multa o debito
- Minacce di chiuderti o bloccarti il conto
- Link che non sembrano autentici, come ad esempio un indirizzo web insolito
- Insolito senso di urgenza o scadenza.

Suggerimento: Se non sei sicuro che un messaggio o una chiamata siano veri, non utilizzare i dettagli di contatto forniti, ma esegui una ricerca su Internet per trovare il numero o l'indirizzo email dell'organizzazione.

Fai attenzione agli amici che hai conosciuto online

I truffatori online spesso entrano in contatto con le persone attraverso i social media. Usano le loro tattiche nelle truffe romantiche o di incontri. Puntano inoltre persone che giocano a giochi online come Words with Friends e Scrabble. Il loro obiettivo è quello di costruire una relazione (non deve essere romantica) per guadagnare la tua fiducia in modo che possano chiederti denaro, informazioni personali, immagini intime o qualcos'altro di valore.

Segni che potrebbe trattarsi di una truffa

Stai attento alle persone che:

- Esprimono rapidamente affetto profondo
- Provano a spostare la conversazione dal sito web in cui ti sei incontrato a un canale di comunicazione più privato, come i messaggi diretti o l'e-mail
- Ti raccontano storie elaborate su problemi economici
- Dicono che vogliono incontrarti ma trovano scuse o chiedono soldi per spostarsi e venire a trovarti
- Fanno domande sul tuo stato finanziario
- Diventano insistenti, più dirette o addirittura aggressive quando non invii denaro
- Sembrano avere incoerenze nel loro profilo online: ad esempio, la loro foto sembra diversa dalla loro descrizione, o dicono che sono andate all'università ma fanno errori di grammatica.

Capita spesso anche che i truffatori si presentino come operatori umanitari o fingano di essere militari o professionisti che lavorano all'estero.

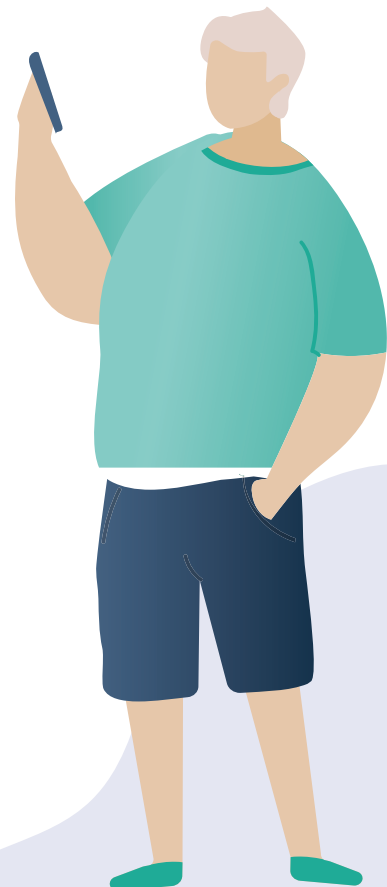
Suggerimento: Fai una ricerca per immagini su alcuni siti come Google (images.google.com) oppure TinEye (tineye.com), per controllare se la persona è chi dice di essere.

In che modo puoi proteggerti

- Non fornire informazioni personali o finanziarie a persone che non hai mai incontrato di persona.
- Non effettuare pagamenti tramite vaglia postale, bonifico bancario, trasferimento internazionale di fondi o valuta elettronica come bitcoin. (È difficile

recuperare i soldi inviati in questo modo, se alla fine si tratta di una truffa.)

- Non accettare di trasportare pacchi a livello internazionale o trasferire denaro per qualcun altro, perché potresti commettere un crimine senza saperlo.
- Non condividere foto intime e non utilizzare webcam in un ambiente intimo.
- Interrompi tutte le comunicazioni se una persona inizia a chiederti un favore o denaro.
- Fai attenzione agli errori di ortografia, agli errori di grammatica e alle incoerenze nelle storie.



Fai attenzione alle truffe sugli investimenti

Coloro che fanno truffe sugli investimenti dedicano molto tempo, sforzi e denaro alla creazione di storie convincenti, siti web elaborati e lucenti per truffare gli australiani più anziani che stanno cercando di far fruttare i loro risparmi.

Come attirano la tua attenzione i truffatori?

Questi sono alcuni dei metodi utilizzati da coloro che fanno truffe sugli investimenti:

- Ti indirizzano a un sito web falso che dichiara cose false su investimenti con prestazioni e rendimenti molto buoni.
- Pubblicano un annuncio o un articolo su un sito di social media come Facebook.
- Ti inviano una richiesta di "amicizia" sui social media facendosi passare per qualcuno che conosci o con cui hai contatti, al fine di accedere alle informazioni del tuo profilo e inviarti offerte di investimento su misura per te.

Segni che potrebbe trattarsi di una truffa

- Il truffatore ti chiama o ti invia email in modo insistente.
- Quando lo chiami fa passare la tua chiamata a varie persone: parli prima con una persona con meno esperienza e poi con una persona con più esperienza che cerca di chiudere l'affare.

- Ti spinge ad agire rapidamente altrimenti perderai l'occasione.
- Dice che non ha un permesso dell'Australian financial services (AFS) o che non gli serve
- Tenta di impedirti di rifiutare l'offerta.



Superannuation (Pensione)

Coloro che fanno truffe sugli investimenti offrono modi semplici e veloci per "sbloccare" anticipatamente la superannuation. Potrebbero chiederti di accettare una storia per garantire il rilascio anticipato dei tuoi fondi e poi, in qualità di consulenti finanziari, ingannano l'azienda che detiene la tua superannuation e fanno sì che i benefici pensionistici siano versati direttamente a loro.

Una volta che ha i tuoi soldi, il truffatore può prelevare ingenti "commissioni" dal fondo rilasciato o lasciarti senza nulla.



Nota bene! Di solito non puoi accedere legalmente alla parte congelata della tua super fino a quando non hai tra i 55 e i 60 anni, a seconda dell'anno in cui sei nato. Esistono alcune eccezioni tra cui gravi difficoltà finanziarie o motivi compassionevoli, ma chiunque offra comunque accesso anticipato alla tua super agisce illegalmente.

Prezzi delle azioni incrementati artificialmente

Coloro che fanno truffe sugli investimenti acquistano azioni di una piccola società a basso prezzo, e poi danno falsi suggerimenti dicendo che la società ha grandi prospettive. Man mano che un numero maggiore di persone investe, il prezzo delle azioni aumenta e i truffatori vendono le loro quote quando il prezzo aumenta al massimo. Poi il prezzo delle azioni scende e gli azionisti restano in possesso delle azioni a valore ridotto.

Truffe con la promozione di persone famose

Coloro che fanno truffe sugli investimenti fanno finta di essere appoggiati da imprenditori o persone famose rispettati e di successo nel tentativo di far credere alle persone che uno schema sia sostenuto da qualcuno di cui si fidano. Queste truffe spesso compaiono come pubblicità online o storie promozionali sui feed dei social media o siti web apparentemente legittimi e affidabili.

In che modo puoi proteggerti

- Diffida delle opportunità che sembrano troppo belle per essere vere.
- Diffida delle pubblicità o delle storie che sono appoggiate da persone famose.
- Non permettere a nessuno di farti pressione.
- Se hai meno di 55 anni, fai attenzione alle offerte che promuovono di poter facilmente accedere ai benefici pensionistici.
- Fai le tue ricerche e cerca consulenza finanziaria o legale affidabile o indipendente.

- Non fornire informazioni personali o finanziarie fino a quando:
 - Non hai verificato se il consulente finanziario e la sua società sono registrati tramite il sito web ASIC asic.gov.au/online-services/search-asics-registers/.
 - Non hai controllato l'elenco ASIC delle società con cui non dovresti fare affari moneysmart.gov.au/scams/companies-you-should-not-deal-with.

Aiuto, sospetto di essere vittima di una truffa

Se pensi di essere vittima di truffa, non ti sentire imbarazzato e non tenerti tutto per te. Ci sono delle cose che puoi fare per risolvere il problema:

- Contatta la tua banca per interrompere qualsiasi ulteriore pagamento al truffatore.
- Contatta ID Care idcare.org se le tue informazioni personali sono state rivelate o utilizzate in modo improprio.
- Per eventuali truffe su Medicare, Centrelink o myGov, chiama Services Australia al numero 1800 941 126 o invia un'email reportascam@servicesaustralia.gov.au.
- Segnala la truffa all'Australian Competition and Consumer Commission su scamwatch.gov.au in modo che possano far sapere ad altre persone come evitarla.

Per tenerti aggiornato sulle ultime truffe da evitare, iscriviti agli avvisi e-mail di Scamwatch scamwatch.gov.au/news/subscribe-to-scam-alert-emails

Scopri con calma Be Connected

Be Connected è un sito web completo con risorse gratuite appositamente progettato per assistere le persone anziane australiane a connettersi online senza correre rischi e a navigare in modo sicuro nel mondo digitale. Il sito è utile anche per le famiglie e le organizzazioni comunitarie che vogliono aiutare i membri più anziani della comunità ad accedere a tutti i vantaggi di Internet.

beconnected.esafety.gov.au

