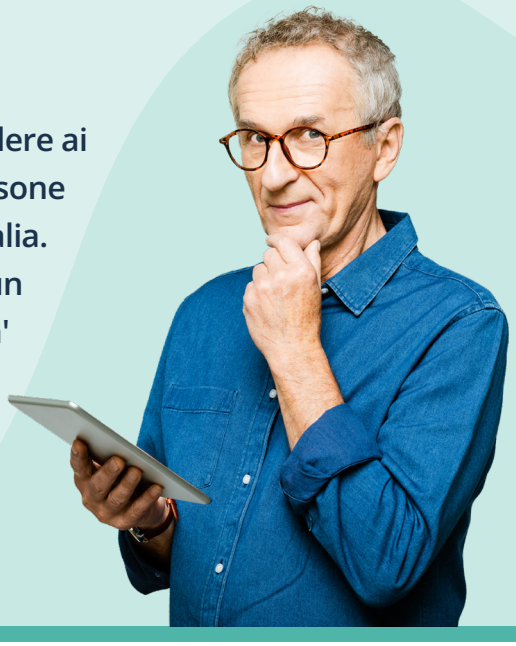
Riepilogo presentazione online

Australian Government

Be Connected
Every Australian online.

Proteggiti dalle truffe



I truffatori adottano tentativi sempre più sofisticati per accedere ai tuoi soldi o dettagli personali. Le truffe prendono di mira persone di qualsiasi background, età e livello di reddito in tutta Australia. Le truffe online sono solitamente eseguite da qualcuno con un profilo falso oppure da un'azienda che finge di far parte di un' organizzazione ben conosciuta. Quindi, anche se Internet può essere un posto meraviglioso da esplorare, vale la pena essere cauti! Stai attento e proteggiti dalle truffe seguendo i nostri consigli.

Proteggi le tue informazioni personali

I truffatori fanno finta di far parte di organizzazioni che conosci e di cui ti fidi come aziende con cui hai contatti, agenzie governative oppure servizi per le truffe per cercare di farti rivelare importanti informazioni personali e finanziarie. Potrebbero contattarti per telefono, email, messaggio di testo oppure attraverso i social media. I truffatori useranno i tuoi dati personali per rubarti soldi o commettere un altro crimine.

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

- Verificare chi sei o aggiornare i tuoi dettagli
- Cliccare su un link
- Dare loro accesso remoto al tuo computer
- Pagare un debito
- Comprare un buono acquisto per pagare una multa
- Trasferire fondi o inviare denaro all'estero.

Segni che potrebbe trattarsi di una truffa

- Email, 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.

Ricorda: i truffatori potrebbero cercare di far leva sui tuoi sentimenti per farti reagire e non darti tempo di pensare attentamente alla situazione. Le loro tattiche potrebbero includere l'utilizzo di minacce o multe, potrebbero dirti che ci sono state delle spese non autorizzate sul tuo conto oppure potrebbero far finta di essere un familiare che ha bisogno di aiuto.

In che modo puoi proteggerti

- Presta attenzione al fatto che i truffatori esistono e considera sempre la possibilità che un messaggio, un'email oppure una chiamata telefonica possa essere una truffa.
- Sappi con chi hai a che fare. Se non sei sicuro se 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.
- Non fornire informazioni personali o finanziarie.
- Non aprire messaggi di testo o finestre pop-up sospette e non cliccare su link o allegati sulle email, eliminali.
- Non rispondere a chiamate relative al tuo computer in cui ti viene chiesto l'accesso remoto, riaggancia, anche se dicono il nome di una compagnia ben conosciuta, come ad esempio Telstra.

Stai attento quando fai amicizia online

I truffatori contattano le persone, solitamente attraverso i social media, siti di appuntamenti oppure addirittura attraverso i giochi online. Saranno molto amichevoli ed interessanti e molto propensi a fare amicizia o ad allacciare una relazione con te. I truffatori possono essere sorprendentemente pazienti. La relazione falsa potrebbe continuare per settimane, oppure addirittura un anno, in modo che possano ottenere la tua fiducia e chiederti denaro, informazioni personali, immagini intime oppure indurti a fare qualcosa di illegale.

Segni che potrebbe trattarsi di una truffa

Stai attento a chi:

- Esprime rapidamente sentimenti profondi e ti contatta spesso
- Non può incontrarti di persona, o ti chiede soldi per spostarsi e venire a trovarti
- Prova a spostare la conversazione dalla piattaforma o app in cui vi siete incontrati a un canale di comunicazione più privato, come i messaggi diretti o le email
- Dice di avere una situazione finanziaria stabile ma ti chiede denaro
- Ti racconta storie elaborate su problemi economici
- Fa domande sul tuo stato finanziario
- Diventa disperato, più diretto o addirittura aggressivo quando non invii denaro
- Sembra avere incoerenze nelle storie e nel profilo online. Ad esempio: la sua foto è diversa dalla descrizione
- Fa errori di ortografia e grammatica
- Dice di lavorare all'estero (ad esempio un operatore di un’organizzazione umanitaria o qualcuno che lavora nell'esercito).

In che modo puoi proteggerti

- Non inviare mai denaro e non dare mai i dettagli della carta di credito, i dettagli dell'account online, oppure copie di documenti personali importanti a qualcuno che non hai incontrato di persona.
- Effettua una ricerca per immagini per aiutarti a determinare se è veramente chi dice di essere. Vai su images.google.com e fai clic sull'icona della fotocamera.
- Sii diffidente quando inizia a parlarti di problemi di denaro o ti dice che ha bisogno di soldi per un'"emergenza".
- Stai attento a cose come gli errori di ortografia e di grammatica, alle incoerenze nelle storie che racconta.
- Non accettare di trasportare pacchi a livello internazionale o trasferire denaro per qualcun altro, in quanto potresti commettere un crimine.
- Non condividere immagini o video intimi. È risaputo che i truffatori ricattano i loro bersagli utilizzando materiale compromettente.
- Interrompi tutte le comunicazioni se una persona inizia a chiederti un favore o denaro.
- Evita qualsiasi accordo con un estraneo che ti chiede un pagamento per vaglia postale, bonifico telegrafico, trasferimento fondi internazionale, carta prepagata o valuta elettronica, come Bitcoin. È difficile recuperare il denaro inviato in questo modo.

Fai attenzione alle truffe relative a investimenti

Le truffe relative a investimenti utilizzano promesse di grossi pagamenti, denaro veloce o profitti garantiti. Diffida sempre di opportunità di investimento che promettono alti profitti con poco rischi o nessun rischio.

Gli australiani perdono più soldi nelle truffe relative a investimenti che in qualsiasi altra truffa. Possono essere difficili da individuare, in quanto i truffatori si impegnano molto a inventare storie convincenti e a creare siti professionali e materiale promozionale. Prima di investire, ottieni sempre consulenza legale o finanziaria indipendente da un consulente finanziario che sia registrato con l'Australian Securities and Investments Commissions (ASIC).

Alcuni dei modi più comuni in cui possono funzionare le truffe relative a investimenti possono essere:

- Contattarti per email o per telefono con un'opportunità speciale di ottenere profitti veloci o garantiti
- Utilizzare la falsa sponsorizzazione di una persona famosa per far sembrare vera la truffa
- Convincerti di accedere alla tua superannuation anticipatamente o come somma forfettaria
- Seminari di investimento (spesso per video online, Zoom o simili) che sono gratuiti o che costano molto.

Superannuation (Pensione)

Le truffe relative alla superannuation offrono di darti accesso anticipato al tuo fondo pensionistico, spesso attraverso un fondo pensionistico autogestito oppure a pagamento. L'offerta potrebbe esserti fatta da un truffatore che si fa passare per un consulente finanziario.

Potrebbe chiederti di concordare una storia per garantire il rilascio anticipato dei tuoi fondi e poi, in qualità di consulente finanziario, inganna l'azienda che detiene la tua superannuation e fa sì che i contributi pensionistici siano versati direttamente a lui. Una volta che ha i tuoi soldi, il truffatore può prelevare ingenti "commissioni" dal fondo rilasciato o lasciarti senza nulla.

Nota: 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. Per maggiori informazioni visita: moneysmart.gov.au/how-super-works/superannuation-scams

Promozioni relative ad azioni e soffiate

I truffatori possono contattarti per email, social media oppure pubblicare un messaggio in un forum per incoraggiarti a comprare azioni in una compagnia che prevedono aumenterà in valore. Il messaggio sembra un'informazione privilegiata e spesso sottolineerà che devi agire rapidamente. Il truffatore sta cercando di farti comprare azioni per far aumentare il prezzo del capitale in modo da poter vendere le azioni che ha già e ottenere un grosso profitto. Il valore delle azioni poi andrà giù drasticamente.

Truffe con la promozione di persone famose

I truffatori utilizzano l'immagine, il nome e le caratteristiche personali di personaggi famosi molto conosciuti senza il loro permesso per indurti a investire in quanto l'investimento è supportato da qualcuno di cui ti fidi. Queste truffe spesso compaiono come pubblicità online o storie promozionali sui feed dei social media o siti web apparentemente legittimi e affidabili.

Campanelli di allarme che indicano una truffa relativa a investimenti

Se vieni contattato improvvisamente per telefono, messaggio di testo, email o messaggio sui social media da qualcuno che ti offre consulenza relativa ad investimenti senza che tu glielo abbia chiesto e:

- Utilizza strategie che ti fanno pressione, ad esempio ti contatta ripetutamente per farti pressione affinché tu prenda una decisione rapida.
- Promette basso rischio con profitti alti o garantiti.
- Non ha un permesso dell'Australian Financial Services (AFS) o dice che non gli serve.
- Ha un prospetto di investimento che non è registrato con l'ASIC.
- Utilizza la promozione o le immagini di persone famose: sono solitamente false. Le persone famose di rado discutono dei loro investimenti o delle loro decisioni finanziarie in pubblico.
- Ti manda su un sito web falso.
- Tenta di impedirti di rifiutare l'offerta.

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-asic-s-registers/
  - Non hai controllato l'elenco ASIC delle società con cui non dovresti fare affari moneysmart.gov.au/companies-you-should-not-deal-with

Consigli preziosi per evitare le truffe

Fermati

- Fermati a riflettere prima di dare del denaro o delle informazioni personali a una persona qualsiasi.
- I truffatori si offriranno di aiutarti o ti chiederanno di verificare chi sei. Fingeranno di far parte di organizzazioni che conosci e di cui ti fidi come ad esempio un'azienda con cui hai contatti, la polizia, il governo oppure un servizio per le truffe.

Pensa

- Chiediti se il messaggio o la chiamata potrebbero essere falsi.
- Non cliccare mai un link in un messaggio e chiedi a un amico o a un familiare fidato cosa farebbero. Contatta le aziende o il governo utilizzando solamente i dettagli di contatto presenti sul loro sito ufficiale o sulla loro app sicura. Se non sei sicuro dì di no, riaggancia oppure elimina.

Proteggi

- Agisci rapidamente se ti sembra che ci sia qualcosa che non va.
- Contatta immediatamente la tua banca se perdi denaro o informazioni personali oppure se noti delle attività insolite sulle tue carte o sui tuoi conti. Chiedi aiuto ad organizzazioni come IDCARE e denuncia il crimine online su ReportCyber. Aiuta gli altri segnalando le truffe su Scamwatch.

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 immediatamente la tua banca o il tuo istituto finanziario per interrompere qualsiasi ulteriore pagamento al truffatore.
- Se sei stato vittima di un crimine informatico e hai perso del denaro online, puoi denunciare il fatto alla polizia per mezzo di ReportCyber oppure visita: cyber.gov.au
- Se sei preoccupato che le tue informazioni personali siano state esposte e utilizzate in modo improprio, contatta il servizio nazionale australiano di assistenza virtuale e per l'identità IDCARE al numero 1300 432 273 oppure visita idcare.org
- Segnala la truffa ad ACCC attraverso la pagina scamwatch.gov.au/report-a-scam. Ci aiuta ad avvertire le persone sulle truffe correnti, a monitorare gli andamenti e a bloccare le truffe dove possibile.
- Diffondi le informazioni ad amici e familiari per proteggerli.

Ricorda: c'è sempre qualcuno che ti può aiutare, sia che si tratti di qualcuno a cyber.gov.au oppure scamwatch.gov.au, o di un amico o un familiare con una preparazione tecnica, o persino di un club informatico di zona.

Per tenerti aggiornato sulle ultime truffe da evitare, iscriviti agli avvisi e-mail di Scamwatch.

Scopri con calma Be Connected

Be Connected è un sito web completo con risorse gratuite appositamente progettato per assistere gli australiani più anziani 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.

visita beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Questo programma è stato sviluppato da eSafety nell'ambito dell'iniziativa Be Connected.