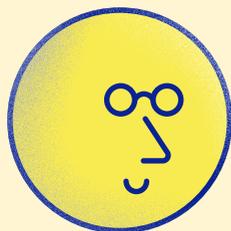


# Come riconoscere ed evitare le truffe



Guida alla protezione dalle  
truffe



Australian Government



National  
Anti-Scam  
Centre



**ScamWatch**  
Stop. Better safe than scammed.

## Acknowledgment of country

L'ACCC riconosce i proprietari e i custodi tradizionali del territorio in tutta Australia e il loro continuo legame con la terra, l'acqua e le comunità. Rendiamo omaggio a loro e alle loro culture, e ai loro Elder passati, presenti e futuri.

Australian Competition and Consumer Commission  
Ngunnawal  
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Commonwealth of Australia 2023

Questa opera è soggetta al diritto d'autore. Oltre a qualsiasi uso consentito dalla Legge sul diritto d'autore del 1968 (*Copyright Act 1968*), tutto il materiale contenuto in quest'opera è fornito con licenza Creative Commons Attribuzione 4.0 Australia, ad eccezione:

- dello stemma del Commonwealth;
- del logo dell'ACCC e dell'AER;
- di qualsiasi illustrazione, diagramma, fotografia o grafico di cui la Commissione australiana per la concorrenza e i consumatori (ACCC) non detiene i diritti d'autore, ma che può essere parte o essere contenuto in questa pubblicazione.

I dettagli delle relative condizioni di licenza sono disponibili sul sito web di Creative Commons, così come il codice legale completo relativo alla licenza CC BY 4.0 AU.

Le richieste e le domande relative alla riproduzione e ai diritti devono essere indirizzate a: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

### Avviso importante

Le informazioni contenute in questa pubblicazione servono solo a titolo informativo. Non costituiscono una consulenza legale o professionale e non devono essere considerate come un'enunciazione della legge in qualsiasi giurisdizione. Poiché si tratta solo di una guida generale, può contenere delle generalizzazioni. In caso di dubbi specifici, si consiglia di rivolgersi a un professionista.

L'ACCC ha compiuto ogni ragionevole sforzo per fornire informazioni aggiornate e accurate, ma non garantisce l'accuratezza, l'attualità o la completezza di tali informazioni.

Coloro che desiderano ripubblicare o utilizzare in altro modo le informazioni contenute nella presente pubblicazione, sono tenuti a verificarne l'attualità e l'accuratezza. Questo dovrebbe essere fatto prima della pubblicazione di ciascuna edizione, in quanto le linee guida dell'ACCC e la relativa legislazione transitoria cambiano frequentemente. Eventuali domande da parte degli interessati devono essere indirizzate a: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24\_24-13

[www.accc.gov.au](http://www.accc.gov.au)

# Indice dei contenuti

<b>Aiuto disponibile</b>	<b>1</b>
<b>Che cos'è una truffa</b>	<b>3</b>
<b>Semplici consigli per individuare ed evitare le truffe</b>	<b>4</b>
<b>Truffe tramite messaggi di testo o SMS</b>	<b>7</b>
<b>Truffe tramite e-mail</b>	<b>11</b>
<b>Truffe telefoniche</b>	<b>15</b>
<b>Truffe tramite siti web</b>	<b>19</b>
<b>Truffe tramite social media, app e applicazioni di messaggistica online</b>	<b>23</b>
<b>Principali truffe da conoscere</b>	<b>27</b>
<b>Dove segnalare le truffe</b>	<b>31</b>
<b>Ulteriore aiuto e supporto</b>	<b>33</b>



## Questa guida è stata redatta dal Centro Nazionale Anti-Truffa (National Anti-Scam Centre) e ti aiuterà a identificare le truffe e a proteggerti dai danni da esse causati.

Una truffa è un crimine e chi la compie è un criminale. Molte persone in Australia vengono truffate perdendo somme di denaro, a volte anche i risparmi di una vita. Le truffe danneggiano la vita delle persone.

Le truffe sono sempre più difficili da individuare, quindi dobbiamo lavorare insieme per fermarle.

Il Centro Nazionale Anti-Truffa (National Anti-Scam Centre) si occupa di tenere gli australiani al sicuro dalle truffe.

Collaboriamo con il governo e le imprese per trovare nuovi modi per impedire ai truffatori di rubare denaro e informazioni personali appartenenti agli australiani. Ecco alcuni dei modi in cui perseguiamo questo obiettivo.

### **Aiutiamo le persone a individuare ed evitare le truffe**

Attraverso Scamwatch, condividiamo informazioni aggiornate sulle truffe e sui modi per proteggersi da esse.

### **Ostacoliamo i truffatori**

Raccogliendo e condividendo le informazioni in ambito governativo e industriale, rendiamo più difficile per i truffatori continuare a commettere crimini e aiutiamo le persone a segnalare le truffe.



# Aiuto disponibile

Se stai leggendo questa guida, è probabile che tu o qualcuno che conosci sia stato truffato. Purtroppo, non siete i soli. Le truffe sono sempre più sofisticate, il che significa che chiunque è a rischio di essere truffato.

Se si è vittima di una truffa, è importante agire rapidamente.

Se hai perso del denaro a causa di un truffatore, contatta la tua banca o la società emittente della carta.

Contatta IDCARE, [1800 595 160](tel:1800595160), [www.idcare.org](http://www.idcare.org).

Le truffe hanno successo perché possono sembrare reali. I truffatori contano sul fatto che i segnali di avvertimento non vengano individuati perché si ha fretta, perché l'offerta proposta sembra vantaggiosa e non la si vuole perdere o perché sembra provenire da qualcuno di cui ci si fida.

## Proteggiti dalle truffe seguendo questi tre consigli:

### Fermati

**Non dare denaro o informazioni personali a nessuno qualora dovessi avere dei dubbi.**



I truffatori si offrono di aiutarti oppure ti chiedono di verificare la tua identità. Fingono di appartenere a organizzazioni che conosci e di cui ti fidi, come fornitori di servizi, la polizia, la tua banca o servizi governativi.

### Controlla

**Poniti la seguente domanda: il messaggio o la telefonata potrebbero essere falsi?**



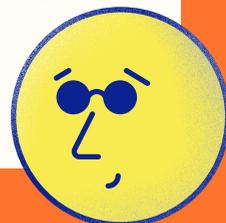
Non cliccare mai su un link contenuto in un messaggio. Contatta le aziende o l'amministrazione pubblica solo utilizzando le informazioni di contatto che trovi sul loro sito web o sulla loro app ufficiale. Se hai dei dubbi, rispondi "no", riaggancia o cancella.

### Segnala

**Agisci rapidamente se qualcosa sembra strano.**



Contatta la tua banca se noti dei movimenti insoliti o se un truffatore si impossessa del tuo denaro o delle tue informazioni. Chiedi aiuto e segnala la truffa a ReportCyber e Scamwatch. Quando segnali una truffa, aiuti tutti gli australiani rafforzando la nostra difesa contro le truffe.



# Che cos'è una truffa

Una truffa avviene quando qualcuno tenta di ingannarti per rubare il tuo denaro o le tue informazioni personali.

Le truffe sono crimini economici gestiti da criminali spesso molto organizzati e sofisticati.

## Le truffe:

- ✓ sono gestite da criminali
- ✓ sembrano reali
- ✓ sono accompagnate da storie credibili
- ✓ esercitano pressioni su di te per indurti a compiere un'azione

## Le truffe NON sono:

- ✗ Hackeraggio del computer
- ✗ Condizioni contrattuali inique
- ✗ Approcci di marketing fastidiosi

È importante ricordare che non tutte le esperienze negative costituiscono una truffa. Può capitare di aver pagato per un prodotto che non si è mai ricevuto o di aver acquistato qualcosa e di aver constatato che la qualità era scarsa. Sebbene ciò sia fonte di delusione, non si tratta necessariamente di una truffa. La legge australiana sui consumatori (Australian Consumer Law) offre protezione ai consumatori australiani per questo tipo di problemi.

Per maggiori informazioni visita il sito [www.accc.gov.au/consumers](http://www.accc.gov.au/consumers)

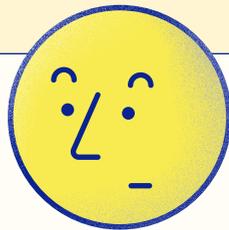
# Semplici consigli per individuare ed evitare le truffe

Le truffe possono capitare a tutti noi. Le truffe funzionano perché i truffatori creano storie credibili per rubare il tuo denaro e ottenere le tue informazioni personali.

I truffatori sono sempre più furbi e sfruttano le nuove tecnologie, i prodotti, i servizi e i grandi eventi per convincerti che le loro truffe sono reali.

Può essere molto difficile individuare una truffa. Ecco alcune situazioni a cui prestare attenzione. A volte i truffatori utilizzano una combinazione di queste tattiche.

- 1. Opportunità di farti guadagnare o risparmiare denaro:** I truffatori cercano di ingannarti facendoti credere che stai concludendo un buon affare o che stai beneficiando di un'offerta incredibile. Ti faranno pressione affinché tu agisca in fretta in modo da non perdere l'occasione. Ricorda che le offerte che sembrano troppo belle per essere vere, di solito lo sono.
- 2. Storie tristi e richieste di aiuto:** I truffatori cercheranno di usare il tuo buon cuore per raggirarti. Condivideranno con te storie di dolore e tragedia e ti spiegheranno perché hanno bisogno del tuo aiuto e del tuo denaro.
- 3. Link e allegati:** I truffatori utilizzano i link per indirizzarti a siti web truffaldini progettati per rubare le tue informazioni e il tuo denaro. I truffatori possono anche invitarti ad aprire



degli allegati. Questi allegati possono installare virus che andranno poi a sottrarre le tue informazioni.

- 4. Pressione ad agire rapidamente:** I truffatori non vogliono che tu prenda tempo e rifletta sulle cose. Vogliono esercitare pressione per indurti ad agire rapidamente. Questa pressione può includere minacce che accadrà qualcosa di grave se non agirai in fretta.
- 5. Richieste di pagamento in modi insoliti o specifici:** I truffatori spesso chiedono di pagare con metodi poco comuni come carte di debito prepagate, carte iTunes o valute virtuali come Bitcoin. Una volta che questo denaro è stato speso, non è possibile recuperarlo.
- 6. Richieste di creazione di nuovi conti o PayID:** I truffatori potrebbero chiederti di creare un nuovo conto bancario o PayID in modo da poter inviare loro denaro (o ricevere denaro da loro). Potrebbero fingere di rappresentare la tua banca e dirti di trasferire il tuo denaro su nuovi conti per tenerlo al sicuro.

Se i truffatori sono riusciti a sottrarti del denaro, proveranno a sottrartene dell'altro. Purtroppo, una vittima di truffa su tre è stata truffata più di una volta. Se hai perso del denaro a causa di una truffa, fai attenzione ai truffatori che ti offrono di aiutarti a recuperare il tuo denaro. Si tratta di un altro tipo di truffa.



# Truffe tramite messaggi di testo o SMS

I truffatori inviano messaggi fingendo di appartenere al governo, alle forze dell'ordine, ad aziende fidate o persino alla tua famiglia o ai tuoi amici.

Questi messaggi avranno un tono urgente e cercheranno di indurti ad agire rapidamente. Spesso contengono un link che ti conduce a un sito web truffaldino. I truffatori possono rubare tutte le informazioni personali inserite in questi siti web truffaldini e utilizzarle per sottrarre denaro o commettere frodi a tuo nome.

Per far sembrare questi messaggi reali, i truffatori copiano o camuffano il loro numero di telefono così da farti pensare che appartengano ad aziende legittime o a persone conosciute.

I messaggi di truffa possono persino apparire nella stessa catena di messaggi reali provenienti da un'organizzazione, rendendoli ancora più difficili da individuare.

## Indicazioni che un messaggio potrebbe essere una truffa

### Il messaggio:

---



Ti chiede di intraprendere un'azione immediata, di effettuare un pagamento o un trasferimento di denaro.

---



Ti chiede di fare clic su un link o di chiamare un numero fornito nel messaggio.

---



Ti chiede di accedere a un account online con il tuo nome utente e la tua password o di fornire altre informazioni personali.

---



Proviene da un familiare o da un amico, il quale comunica che i suoi dettagli di contatto sono cambiati.

---



Minaccia di interrompere un servizio o di esigere un addebito se non intervieni.

---



Suggerisce che tu o i tuoi account siete stati vittima di hackeraggio oppure coinvolti in una frode.

---



Suggerisce che c'è un problema con un pagamento o con la consegna di un pacco.

---

## Consigli per proteggersi dalle truffe tramite messaggi

---

1. Se qualcuno che conosci invia un messaggio per dire che ha un nuovo numero di telefono:



- a. prova a chiamarlo al suo numero esistente, e
- b. inviagli un messaggio al nuovo numero con una domanda di cui solo lui conosce la risposta, per verificare che sia chi dice di essere.



2. Non cliccare mai sui link contenuti nei messaggi.



3. Se un messaggio rimanda a un sito web, non cliccare sul link. Invece, cerca tu stesso il sito web online o utilizza l'app ufficiale dell'organizzazione.



4. Non rispondere a un messaggio di testo utilizzando il numero di telefono fornito.



5. Richiama l'organizzazione o la persona su un numero di telefono che hai individuato autonomamente, ad esempio dal sito web dell'organizzazione.



# Truffe tramite e-mail

I truffatori inviano e-mail che fingono di provenire dal governo, dalle forze dell'ordine e dalle aziende. Fanno sembrare la questione urgente per indurirti ad agire rapidamente.

I truffatori utilizzano lo stesso logo e un indirizzo e-mail simile a quello dell'organizzazione reale. I truffatori possono anche copiare o camuffare il proprio indirizzo e-mail dietro l'indirizzo di un'organizzazione o di un'azienda per far sembrare l'e-mail truffaldina più reale.

## Indicazioni che un'e-mail potrebbe essere una truffa

### L'e-mail:

---



Richiede un pagamento, ma i dati del conto sono nuovi o sono cambiati rispetto all'ultimo pagamento effettuato.

---



Ti chiede di accedere a un account online con il tuo nome utente e la tua password o di fornire altre informazioni personali.

---



Era inaspettata e include un allegato e un invito ad aprirlo.

---



Ti chiede di confermare i tuoi dati bancari per ricevere un rimborso o del denaro inaspettato.

---



Dichiara di avere informazioni su di te o immagini che ti ritraggono e minaccia di diffonderle.

---



Si offre di aiutarti a recuperare denaro o a ottenere un risarcimento per una violazione dei dati o un furto d'identità.

---

## Consigli per proteggersi dalle truffe tramite e-mail

---

1. Controlla che l'e-mail sia reale compiendo una di queste azioni:



- a. contatta direttamente la persona o l'organizzazione utilizzando i dettagli di contatto che hai reperito autonomamente, ad esempio dal sito web dell'organizzazione, oppure,
  - b. accedi alle informazioni che riguardano un'organizzazione tramite le app ufficiali (mai tramite un link).
- 



2. Interrompi immediatamente i contatti con chiunque cerchi di minacciarti o intimidirti.
- 



3. Non fornire mai dati personali né inviare denaro a chi ti offre:
    - a. un risarcimento o un aiuto per rimetterti in sesto in seguito a una precedente truffa o violazione dei dati, oppure,
    - b. vincite, premi o eredità.
- 



4. Utilizza l'autenticazione a più fattori qualora possibile. Questo fornisce un ulteriore livello di protezione e implica che un truffatore debba conoscere la tua password di posta elettronica e un numero pin inviato al tuo telefono per ottenere l'accesso al tuo account di posta elettronica.
-



# Truffe telefoniche

I truffatori chiamano affermando di appartenere a organizzazioni note. Può trattarsi di organizzazioni governative, forze dell'ordine, società di investimento e legali, banche e fornitori di servizi di telecomunicazione.

Fanno sembrare la questione urgente per indurti ad agire rapidamente. Potrebbero tentare di convincerti a fornire i tuoi dati personali o del conto corrente, o di accedere al tuo computer.

La persona che chiama potrebbe essere già in possesso di dati su di te, come il tuo nome o il tuo indirizzo, facendo così sembrare la telefonata reale.

## Indicazioni che una telefonata potrebbe essere una truffa

### La persona che chiama:

---



Ti chiede di effettuare un pagamento o di spostare del denaro su un nuovo conto.

---



Ti chiede di fornire la tua password, il tuo pin, il tuo codice univoco o altre informazioni di sicurezza.

---



Ti chiede di fornire dati finanziari, come quelli relativi alla carta di credito o al conto corrente.

---



Ti chiede di completare un'azione sul tuo cellulare o computer, come installare un software o accedere a un account protetto.

---



Dichiara di far parte delle forze dell'ordine e ti minaccia di arresto immediato o di deportazione.

---



Dice che la tua banca o altri conti online sono stati violati o coinvolti in una frode.

---

## Consigli per proteggersi dalle truffe telefoniche

---

1. Verifica che la chiamata sia reale compiendo una di queste azioni:



- a. contatta direttamente la persona o l'organizzazione utilizzando i dettagli di contatto che hai reperito autonomamente, ad esempio dal sito web dell'organizzazione, oppure,
- b. accedi alle informazioni che riguardano un'organizzazione tramite le app ufficiali (mai tramite un link).



2. Se non hai la certezza a riguardo dell'identità della persona che chiama o se questa persona ti minaccia o ti intimidisce, riaggancia immediatamente.



3. Non installare mai un software che permetta a qualcuno di accedere al tuo computer o dispositivo.



4. Puoi anche decidere di ignorare le chiamate provenienti da numeri che non conosci o lasciare che le chiamate passino alla segreteria telefonica.



### Buono a sapersi!

Anche se disponi di un numero privato o hai effettuato l'iscrizione al registro delle chiamate indesiderate, puoi comunque ricevere telefonate truffaldine.



# Truffe tramite siti web

I truffatori possono fingere di essere chiunque online, compresi il governo, un'azienda reale, personaggi famosi o i tuoi amici o familiari.

Possano creare siti web falsi per sembrare marchi famosi. Possano impersonare personaggi famosi e far credere che stiano approvando determinati prodotti o servizi. Questi siti web possono contenere recensioni false per indurti a fidarsi di loro.

Potresti vedere finti banner pubblicitari o finestre pop-up che contengono finti avvisi o messaggi di errore quando stai navigando online.

## Indicazioni che un sito web potrebbe essere una truffa:

### Il sito web:

---



Offre articoli in vendita a prezzi significativamente più bassi del solito o rispetto ad altri siti.

---



Ti informa su un modo per fare soldi facili e veloci con pochi rischi o sforzi.

---



Contiene un avvertimento urgente o un messaggio di errore che chiede di cliccare su un link.

---



Chiede di effettuare pagamenti in modi insoliti o specifici, ad esempio con carte regalo o criptovalute come Bitcoin.

---



Include solo recensioni positive.

---

## Consigli per proteggersi dalle truffe tramite siti web

---



1. Confronta i prezzi. Se un'offerta sembra troppo bella per essere vera, è probabile che lo sia.
- 



2. Informati sull'organizzazione o sulla persona con cui hai a che fare prima di effettuare pagamenti o di fornire le tue informazioni personali.
- 



3. Non fidarti delle recensioni pubblicate sul sito web in questione. Cerca online il nome del sito web o dell'azienda e la parola "truffa" o "recensioni".
- 



4. Se sullo schermo compare un messaggio di avviso o di errore, non cliccarci sopra, ma vai direttamente all'applicazione a cui si riferisce per verificare se è reale.
- 



5. Mantieni aggiornato il dispositivo che utilizzi per gli acquisti online attivando gli "aggiornamenti automatici" per il sistema operativo e le applicazioni.



### Buono a sapersi!

Consigli pratici per proteggersi online sono disponibili su [www.cyber.gov.au](http://www.cyber.gov.au).



# Truffe tramite social media, app e applicazioni di messaggistica online

Se qualcuno che non conosci ti contatta sui social media, su una piattaforma di messaggistica come WhatsApp o WeChat, o tramite un'app, potrebbe trattarsi di una truffa.

I truffatori che fingono di essere qualcun altro spesso utilizzano una fotografia reale della persona o il logo ufficiale dell'organizzazione che fingono di essere, per rendere la truffa più difficile da individuare.

I truffatori sui social media creano profili falsi e fingono di appartenere al governo, a un'azienda reale, a un datore di lavoro, a una società di investimento o fingono persino di essere un amico, un familiare o una persona con cui si potrebbe condividere un interesse romantico.

Possono impersonare personaggi famosi e far credere che stiano promuovendo beni o servizi.

I truffatori possono conoscere molti dettagli su di te che hanno ottenuto dalle informazioni che condividi sui tuoi account social. Possono utilizzare queste informazioni per indovinare le password dei tuoi account o per tentare di truffarti nuovamente.

## Indicazioni che si potrebbe trattare di una truffa tramite social media o app

### Il profilo social o l'app:

---



Ti informa su un modo per fare soldi facili e veloci con pochi rischi o sforzi.

---



Ti invita a partecipare a un concorso o a un'offerta a tempo limitato.

---



Ti invita a spostare una conversazione dall'app che stai utilizzando, ad esempio un'app di incontri, a una chat privata o a una conversazione tramite e-mail.

---



Suggerisce che un personaggio famoso approva o sostiene un prodotto o un servizio.

---



Sostiene che qualcuno comprerà qualcosa che hai messo in vendita senza averlo visto prima e a un prezzo elevato.

---



Minaccia di condividere una tua foto privata a meno che tu non decida di pagare una somma di denaro.

---



Ti contatta per offrirti un lavoro.

---



### **Buono a sapersi!**

Consigli su come rimanere al sicuro sulle diverse piattaforme di social media sono disponibili su [www.esafety.gov.au](http://www.esafety.gov.au).

## Consigli per proteggersi dalle truffe tramite social media e app



1. Verifica se il profilo potrebbe essere falso. L'account è attivo? Quanti amici/follower ha e quanto spesso posta online?



2. Cerca il nome del profilo online insieme alla parola "scam" (truffa).



3. Non accettare mai un lavoro che ti è stato offerto senza un colloquio o una discussione sulla tua esperienza, sulla tua idoneità e sulle tue referenze. Effettua una ricerca sul selezionatore e sull'azienda o sulla persona che sta offrendo la posizione. Contatta l'agenzia di collocamento tramite i numeri di telefono reperiti tramite una ricerca indipendente su internet. Non effettuare pagamenti in anticipo al fine di assicurarti un lavoro.



4. Accetta consulenze di investimento solo da chi è in possesso di una licenza australiana per i servizi finanziari e controlla che una società o un sito web non siano citati nel portale di allerta per gli investitori dell'Organizzazione internazionale delle commissioni sui valori mobiliari (International Organization of Securities Commission, IOSCO).



5. Non dare mai denaro a una persona che hai conosciuto solo online. I truffatori spesso dicono di vivere all'estero e di non poterti incontrare di persona.



6. Non inviare mai foto intime a qualcuno che hai conosciuto solo online.

Per ulteriori informazioni sulle truffe, compresi altri modi in cui i truffatori potrebbero contattarti, ad esempio di persona o per posta, visita [Scamwatch](#).



# Principali truffe da conoscere

Ecco alcuni dei tipi di truffa più comuni di cui bisogna essere a conoscenza. Puoi trovare maggiori informazioni su ciascuno di questi tipi di truffa, compresi i segnali di avvertimento e le misure per proteggerti, sul sito web di [Scamwatch](#).

## Truffe di impersonificazione

I truffatori ti ingannano facendoti credere di provenire da organizzazioni fidate come la polizia, il governo, le banche e aziende ben conosciute. Possono anche fingere di essere un tuo amico o un tuo familiare. I truffatori cercano informazioni su di te inviando e-mail o messaggi di phishing. Queste e-mail e messaggi sono progettati per rubare le tue informazioni. Cercano di persuaderti a fornire i tuoi dati personali fingendo di provenire da un'organizzazione ufficiale o da qualcuno che conosci e di cui ti fidi.

I truffatori utilizzano la tecnologia per far sembrare le loro chiamate o i loro messaggi provenienti da un numero di telefono legittimo. Possono far apparire i messaggi di testo nella stessa catena di conversazione come se fossero messaggi autentici provenienti da un'organizzazione.

## Truffe di investimento

I truffatori si avvalgono di un marketing convincente e delle nuove tecnologie per far sembrare la loro proposta di investimento troppo bella per non essere presa in considerazione. Promettono grandi guadagni con un rischio minimo o nullo. Spesso utilizzano tattiche di pressione per indurti ad agire in fretta, in modo da poter sottrarti del denaro.

## **Truffe che riguardano il lavoro e l'impiego**

I truffatori offrono lavori ben pagati con poco sforzo. Fingono di assumere per conto di aziende di alto profilo e piattaforme di shopping online. A volte, il lavoro proposto non esiste nemmeno. I truffatori si spacciano anche per note agenzie di collocamento. Il loro obiettivo è rubare il tuo denaro e le tue informazioni personali. Potrebbero chiederti di pagare un anticipo per poter cominciare a lavorare per loro.

## **Truffe che riguardano prodotti e servizi**

I truffatori si fingono acquirenti o venditori con lo scopo di sottrarre il tuo denaro. Creano siti web o profili falsi su siti web legittimi al fine di offrire prodotti o servizi a prezzi stracciati. Pubblicano annunci e recensioni falsi. Possono utilizzare loghi rubati, un nome di dominio .com.au e un Australian Business Number (ABN) in maniera fraudolenta. Queste truffe sono difficili da riconoscere.

I truffatori si spacciano anche per aziende che conosci e di cui ti fidi per inviarti fatture false. Possono anche modificare i dettagli di fatture legittime in modo che i clienti finiscano per pagare il truffatore anziché il vero fornitore.

## **Truffe sentimentali**

I truffatori utilizzano la promessa di amore, appuntamenti o amicizia per sottrarre del denaro. Fanno di tutto per convincerti che la relazione è reale e ti manipolano affinché tu dia loro del denaro.

I truffatori ti trovano sui social media, sulle app e sui siti web di incontri o di gioco. Potrebbero anche inviarti messaggi di testo o e-mail. Si nascondono dietro profili e identità false, a volte di persone famose. Una volta che avranno acquisito la tua fiducia, fingeranno di trovarsi in una situazione di "emergenza" e chiederanno il tuo aiuto. Spesso si tratta di richieste di denaro o di altri prodotti.

## **Truffe contenenti minacce o estorsione**

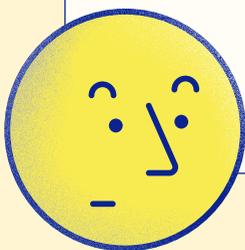
I truffatori fingono di appartenere a un'organizzazione affidabile e affermano che è necessario pagare del denaro per scongiurare un avvenimento indesiderato. Possono minacciarti di arresto, espulsione o persino di provocare dei danni fisici qualora non accetti di effettuare un pagamento immediatamente.

Possono anche ricattarti minacciando di condividere foto o video contenenti immagini di nudo a meno che non decidi di inviare loro del denaro.

## **Truffe che offrono denaro inaspettato**

I truffatori cercano di convincerti che ti è dovuto del denaro o che hai diritto a vincite in denaro che non ti aspettavi di ricevere.

Il truffatore ti chiederà di pagare una commissione o di fornire i tuoi dati bancari o i tuoi dati identificativi prima di poter riscuotere il denaro o le vincite. Purtroppo, nessuno elargisce soldi in maniera gratuita.





# Dove segnalare le truffe

Stiamo cercando di rendere l'Australia un bersaglio più difficile per i truffatori, aumentando la consapevolezza su come riconoscere, evitare e denunciare le truffe.

Condividiamo le informazioni ricavate dalle segnalazioni di truffa e collaboriamo con il governo, le forze dell'ordine e il settore privato per interrompere e prevenire le truffe.

Aiuta gli altri segnalando il caso a Scamwatch. Segnala la tua esperienza di truffa tramite il modulo di segnalazione sul sito web di Scamwatch [www.scamwatch.gov.au](http://www.scamwatch.gov.au).

Ricorda che se sei vittima di una truffa, è importante che tu agisca rapidamente.

- Se hai perso del denaro a causa di un truffatore, contatta la tua banca o la società emittente della carta.
- Contatta ID CARE: 1800 595 160 | [idcare.org](http://idcare.org)



# Ulteriore aiuto e supporto

Essere vittima di una truffa può essere un'esperienza traumatizzante. È importante ricordare che può succedere a chiunque e che è possibile ricevere aiuto e supporto.

Se tu o una persona che conosci avete subito una truffa, parlane con qualcuno. È possibile chiedere supporto alla famiglia, agli amici, al medico di famiglia o a uno dei seguenti servizi di assistenza.

**Lifeline: 13 11 14 | [lifeline.org.au](https://lifeline.org.au)**

oppure utilizza la chat online di supporto in momenti di crisi (24 ore al giorno, 7 giorni alla settimana)

---

**Beyond Blue: 1300 22 4636 | [beyondblue.org.au](https://beyondblue.org.au)**

oppure utilizza la chat online (24 ore al giorno, 7 giorni alla settimana)

---

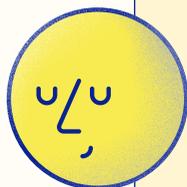
**Kids Helpline: 1800 55 1800 | [kidshelpline.com.au](https://kidshelpline.com.au)**

(24 ore al giorno, 7 giorni alla settimana)

L'impatto finanziario delle truffe può essere devastante e sconvolgerti la vita.

Se ti trovi in difficoltà finanziarie, puoi parlare con un consulente finanziario attraverso la **National Debt Helpline:**

**1800 007 007** dalle 9:30 alle 16:30 dal lunedì al venerdì  
oppure accedi alla chat dalle 9:00 alle 20:00 dal lunedì al venerdì



[scamwatch.gov.au](https://scamwatch.gov.au)