AUSTRALIAN COMPETITION & CONSUMER COMMISSION

Il Libretto Nero delle Truffe

Una guida in formato tascabile per identificare, evitare e proteggersi dalle truffe

Il Libretto Nero delle Truffe

Una guida in formato tascabile per identificare, evitare e proteggersi dalle truffe

ISBN 978 1 920702 00 7

Australian ompetition and onsumer ommission
23 Marcus larke Street, anberra, Australian apital Territory, 2601

A 12/16_1129

www.accc.gov.au

Contenuti

Introduzione

Ogni anno, le truffe costano agli australiani, alle imprese e all'economia centinaia di milioni di dollari e causano danni psicologici alle vittime e alle loro famiglie.

Il modo migliore per proteggersi è attraverso la consapevolezza e l'educazione. Questa nuova edizione del Libretto nero delle truffe è stata presentata dall' agenzia nazionale per la protezione dei consumatori (Australian ompetition and onsumer ommission) (A),.

Il libretto nero delle truffe è riconosciuto a livello internazionale come uno strumento importante affinché i consumatori e le piccole imprese possano riconoscere le truffe tra cui:

- le truffe più comuni a cui prestare attenzione
- i diversi modi con cui i truffatori possono contattarvi
- i modi con cui i truffatori vi ingannano
- i segnali di pericolo
- come proteggersi e
- dove trovare aiuto.

Il libretto nero delle truffe è disponibile online al sito:

www.accc.gov.au/littleblackbookofscams.

Proteggetevi—Iscrivetevi a Scamwatch

Per anticipare i truffatori e saperne di più, visitate il sito web Scamwatch di A - www.scamwatch.gov.au - dove potete registrarvi per ricevere notifiche gratuite via email sulle nuove truffe ai danni di consumatori e piccole imprese. Potete anche seguire Scamwatch su Twitter su @scamwatch_gov or http://twitter.com/scamwatch_gov.

Le truffe migliori da evitare

Tutti sono soggetti alle truffe quindi tutti hanno bisogno di informazioni su come riconoscerle ed evitare di essere truffati. Alcune persone pensano che solo gli ingenui e gli avidi siano vittime di truffe. La verità è che i truffatori sono intelligenti e se non state attenti, potreste cascarci anche voi

Avete ricevuto un'offerta che sembra troppo bella per essere vera, forse una telefonata per aiutarvi a riparare il computer o una minaccia se non pagate soldi che non dovete, un avviso dalla vostra banca o dal vostro fornitore di telecomunicazioni su un problema con il vostro account o anche un invito a "fare amicizia" o connettervi online? I truffatori sanno come prendervi per ottenere ciò che vogliono.

Stanno diventando sempre più intelligenti, stanno al passo coi tempi per sfruttare le nuove tecnologie, i nuovi prodotti, servizi e gli eventi più importanti per creare storie credibili che vi convinceranno a cedere loro denaro o i vostri dati personali.

Tuttavia, grazie alle decine di migliaia di segnalazioni di truffe ricevute ogni anno, l'A ha preparato un elenco di truffe comuni per rivelare i segreti e le tattiche che i truffatori non vogliono che voi conosciate.

Truffe di appuntamenti e incontri romantici

Le truffe per appuntamenti e incontri romantici costano agli australiani vari milioni ogni anno e possono rovinare individui e famiglie.

Come funziona la truffa

I truffatori di **incontri romantici** creano profili falsi su siti di incontri legittimi, app di cellulari o piattaforme di social media come Facebook che utilizzano foto e identità spesso rubate ad altre persone. Usano questi profili per cercare di stabilre una relazione con voi che può durare mesi o anche anni, al fine di prendere i vostri soldi. Il truffatore chiederà soldi per essere aiutato a seguito di malattia, infortunio, spese di viaggio o una crisi familiare. Sono senza cuore e vi mentiranno per approfittare della vostra bontà.

I truffatori di solito sono all'estero e hanno una scusa per spiegare perché vi si trovano, come ad es. essere in servizio militare, lavorare come ingegnere o prendersi cura di un amico o un parente. Non sono mai chi dicono di essere e quelli astuti possono persino inviare piccoli regali. Questa è solo una parte del loro grande piano per ottenere successivamente ancora più soldi da voi.

Proteggetevi

- Non inviate mai denaro e non fornite i vostri dati personali a qualcuno che avete incontrato solo online.
- Fate attenzione se un ammiratore online chiede di comunicare al di fuori del sito di incontri o della piattaforma di social media dopo solo pochi 'contatti' o conversazioni: potrebbe trattarsi di un truffatore.
- Fate una ricerca delle immagini del vostro ammiratore per determinare se è davvero chi dice di essere. Potete utilizzare i servizi di ricerca di immagini come Google o TinEye.
- Siate cauti quando condividete foto o video intimi online. I truffatori sono noti per ricattare i loro obiettivi usando immagini o video di voi che non vorreste fossero viste da nessun altro.

Truffe di investimenti

'Investimento senza rischi' o opportunità di sfortuna?

Come funziona la truffa

Le truffe di investimenti appaiono sotto molte forme, tra cui l'acquisto di criptovaluta, il trading di opzioni binarie, le iniziative imprenditoriali, i piani pensionistici, i fondi gestiti e la vendita o l'acquisto di azioni o proprietà. I truffatori mascherano le "opportunità" con depliant e siti web dall'aspetto professionale per celare le loro operazioni fraudolente. Spesso iniziano con una telefonata o un'e-mail inaspettata e offrono un'opportunità "da non perdere", "ad alto rendimento" o "garantita". Il truffatore di solito opera dall'estero e non è in possesso di licenza dei servizi finanziari australiani.

Le truffe del software di previsione informatica promettono di prevedere con precisione i movimenti del mercato azionario, i risultati delle corse di cavalli, gli eventi sportivi o le lotterie. Sono semplicemente una forma di gioco mascherato sotto forma di investimenti. La maggior parte degli schemi o dei programmi non funziona e gli acquirenti non possono recuperare i loro soldi. In molti casi il fornitore semplicemente scompare.

Le truffe di pensione offrono l'accesso anticipato al vostro fondo pensionistico, spesso tramite un fondo pensionistico autogestito o a pagamento. Il truffatore potrebbe chiedervi di acconsentire a una storia inventata per permettere il rilascio anticipato dei vostri soldi e poi, agendo in veste di vostro consulente finanziario, inganna il vostro fondo pensionistico e si fa pagare direttamente la vostra pensione. Una volta ricevuti i vostri soldi, il truffatore può prendersi ingenti "somme" oppure lasciarvi senza niente.

Proteggetevi

- Non permettete a nessuno di spingervi a prendere decisioni in merito ai vostri soldi o investimenti, specialmente se l'offerta è venuta fuori dal nulla.
- Prima di separarvi dai vostri soldi, fate le ricerche sulla società di investimento e controllate www.moneysmart.gov.au per verificare se hanno una licenza di servizi finanziari australiani. Chiedetevi: se uno sconosciuto conosce il segreto per fare soldi, perché mai condividerlo?

Se siete in età pensionabile, fate attenzione alle offerte che promuovono un facile accesso ai vostri benefici pensionistici. Se accedete illegalmente alla vostra pensione in anticipo, potreste essere penalizzati dalle leggi fiscali.

Truffe con minacce e multe

Se un'autorità governativa o un'azienda fidata vi sta chiedendo di pagare, fermatevi, pensate e ricontrollate.

Come funziona la truffa

Invece di offrire un premio, denaro o rimborso, queste truffe utilizzano minacce progettate per spaventarvi e farvi sborsare soldi. Il truffatore potrebbe chiamarvi e minacciarvi di venire **arrestati** o inviarvi una e-mail con cui chiede il pagamento per una **multa di eccesso di velocità**, un **debito dell'ufficio delle imposte** o una **bolletta non pagata**.

Durante la telefonata, i truffatori vi spingono a pagare immediatamente e vi dicono che manderanno la polizia a casa vostra se vi rifiutate di farlo. I truffatori sono noti per colpire persone vulnerabili nella nostra comunità, come i migranti appena arrivati. Fingono di essere funzionari del Dipartimento dell'Immigrazione e minacciano le vittime di **espulsione,** a meno che non vengano pagate le tasse per correggere gli errori nei loro visti. Una truffa molto simile si verifica quando il truffatore finge di essere impiegato dell'ufficio delle imposte australiano e dice alle loro vittime che hanno una fattura fiscale in sospeso.

I truffatori fingono anche di essere **aziende di fiducia** come la vostra banca o il fornitore di gas, elettricità, acqua o telefonia. Vi minacceranno di cancellare il servizio o di addebitare una penale eccessiva se non pagate immediatamente la bolletta.
A volte possono impersonare un'azienda come l'ufficio postale australiano (Australia Post) che afferma di avere un articolo da ritirare altrimenti vi verrà addebitata una commissione per ogni giorno che non pagate. In ogni caso, cercano di farvi preoccupare e di farvi agire senza riflettere e verificare che la storia sia vera.

Se la truffa viene inviata tramite e-mail, è probabile che includa un allegato o un collegamento a un sito web fasullo ove vi verrà chiesto di scaricare la fattura della "bolletta", "multa" o dei "dettagli di consegna". L'apertura dell'allegato o il download del documento comporterà l'infezione del computer da parte di malware (vedi pagina 16).

Proteggetevi

- Non fatevi mettere sotto pressione da una persona minacciosa al telefono. Fermatevi, riflettete e controllate se quanto dicono è vero.
- Un'agenzia governativa o una società fidata non vi chiederà mai di pagare con metodi insoliti come buono regalo, bonifici bancari o Bitcoin.
- Verificate l'identità del contatto chiamando direttamente l'organizzazione interessata, li potete trovare tramite una fonte indipendente come una guida telefonica, una vecchia fattura o una ricerca online.
- Non utilizzate i dati di contatto forniti nelle e-mail o durante le telefonate. Come ribadito, cercateli tramite una fonte indipendente.

Truffe di denaro inaspettato

Se vi viene chiesto di effettuare pagamenti prima di ricevere merci o denaro, pensateci due volte.

Come funziona la truffa

I truffatori vi diranno improvvisamente che avete diritto a soldi, gemme preziose, oro o azioni di valore ma che dovrete effettuare **pagamenti anticipati** per ottenerli. Non riceverete mai ciò che vi è stato promesso e ci sarà sempre una scusa per cui dovrete pagare di più. Se pagherete, perderete i vostri soldi.

Le truffe di rimborso o di restituzione soldi avvengono quando un truffatore vi dice che vi devono dei soldi a seguito di tasse pagate in eccesso, spese bancarie o qualche sorta di risarcimento. Tuttavia, prima che voi possiate ricevere i soldi, vi viene chiesto di pagare una piccola tassa amministrativa.

on **le truffe di eredità**, i truffatori si presentano come avvocati, banchieri o funzionari stranieri e vi dicono che avete diritto a un'ingente eredità oppure vi offrono parte di uno schema dato che avete lo stesso nome di una persona deceduta. Spesso utilizzano documenti dall'aspetto ufficiale e vi chiedono di effettuare pagamenti per tasse e imposte prima di poter ricevere l'eredità. Possono anche chiedere i vostri dati personali per compilare 'documenti ufficiali'. iò significa che potrebbero rubarvi l'identità oltre ai vostri soldi.

Le truffe che vengono comunemente chiamate **'truffe nigeriane',** possono provenire dall' Africa occidentale, così come da qualsiasi parte del mondo. Si tratta di truffatori che affermano di aver bisogno del vostro aiuto per assicurarsi una grande fortuna

che stanno cercando disperatamente di trasferire fuori dal loro paese. Possono rivendicare che la fortuna è un gruzzolo di denaro nascosto, oro o beni abbandonati da un governo o funzionario corrotto e se accettate di riceverli vi daranno una grande quota quando sarà sicuro farlo. ome tutti questi tipi di truffe, vi diranno che prima è necessario pagare le tasse, le spese bancarie o le tasse per i controlli antiterrorismo e antiriciclaggio prima che possano inviarvi i soldi.

Queste truffe provengono solitamente dall'estero e richiedono il pagamento tramite vaglia postale, ma possono anche richiedere bonifici bancari o altri metodi di pagamento.

Se ci cascate, non riceverete mai nulla dal truffatore e perderete i soldi inviati.

Proteggetevi

- Ricordate che non ci sono schemi di guadagno facile: se sembra troppo bello per essere vero probabilmente lo è.
- Evitate qualsiasi accordo con uno sconosciuto che richiede il pagamento anticipato tramite vaglia postale, bonifico bancario, trasferimento internazionale di fondi, carta prepagata o valuta elettronica. È raro recuperare i soldi inviati in questo modo.
- Se una e-mail indesiderata sembra sospetta, basta eliminarla. Non cliccate su alcun link.
- I dipartimenti governativi, le banche o le aziende di fornitura non vi contatteranno mai per chiedervi di pagare in anticipo al fine di richiedere una commissione o un rimborso.
- In caso di dubbi, verificate l'identità del contatto in modo indipendente. Non utilizzate i dati di contatto forniti nel messaggio che vi è stato inviato: cercate i dati di contatto corretti tramite una fonte indipendente come una guida telefonica o una ricerca online.
- Effettuate una ricerca online utilizzando il testo esatto dell'offerta - in questo modo è possibile identificare molte frodi.

Truffe premio e lotteria

Non fatevi ingannare da una vincita a sorpresa – sarà solo il truffatore a portare a casa il premio.

Come funziona la truffa

Queste truffe cercano di indurvi a dare soldi in anticipo o a fornire i vostri dettagli personali per ricevere un premio da una lotteria, un concorso o una competizione a cui non vi siete mai iscritti. I truffatori affermano che è necessario pagare tariffe o tasse prima che le vostre "vincite" o i vostri premi possano essere versati. Potrebbe anche essere necessario chiamare o inviare un SMS a un numero di telefono a tariffa maggiorata per richiedere il premio.

Gli imbrogli con gratta e vinci includono la ricezione di posta contenente depliant lucidi e svariati gratta e vinci, uno dei quali sarà il vincitore. Per renderlo più credibile, sarà spesso il secondo o il terzo premio. Quando chiamate per richiedere il premio, i truffatori vi chiederanno di pagare delle tariffe o tasse prima di poter ricevere la vostra vincita.

Le truffe della lotteria possono utilizzare i nomi delle lotterie reali all'estero per informarvi che avete vinto denaro, anche se non vi siete mai iscritti. I truffatori normalmente chiedono tariffe o tasse per sbloccare i fondi. Vi diranno anche che hanno bisogno dei vostri dati personali per dimostrare di essere il vincitore giusto, ma poi useranno queste informazioni per rubarvi l'identità o prelevarvi denaro dal conto bancario.

Voucher e buoni regalo falsi coinvolgono truffatori che vi inviano un messaggio via email, di testo o sui social media con cui vi informano che avete vinto un buono regalo per un noto commerciante ma che dovete fornire alcuni dettagli prima di poterlo utilizzare. Questo è un tentativo di ottenere informazioni personali che possono essere utilizzate per il furto di identità o per colpirvi con un'altra truffa. Anche offerte come queste sono note per infettare i vostri dispositivi elettronici (vedi pagina 17).

Le truffe di premi di viaggio riguardano truffatori che vi dicono che avete vinto una vacanza o un biglietto aereo. In effetti, ciò che avete effettivamente vinto è la possibilità di acquistare alloggi o buoni di volo. Questi voucher di viaggio hanno spesso tariffe e condizioni aggiuntive oppure possono essere falsi e privi di valore. Allo stesso modo, i truffatori potrebbero offrirvi fantastici pacchetti scontati di vacanze che semplicemente non esistono.

Proteggetevi

- Ricordate: non potete vincere denaro con una lotteria o una competizione se non vi siete iscritti.
- Le competizioni e le lotterie non richiedono il pagamento di una commissione per raccogliere le vincite - effettuate una ricerca online utilizzando il testo esatto dell'offerta. Questo può aiutarvi a confermare che si tratta di una truffa.
- Pensateci due volte prima di chiamare o inviare messaggi di testo a un numero di telefono che inizia con "19" – le chiamate verranno addebitate a tariffe altissime.

Truffe di acquisti online, annunci e aste

I truffatori amano anche la facilità dello shopping online.

Come funziona la truffa

I consumatori e le aziende acquistano e vendono sempre più online. Sfortunatamente, i truffatori amano adescare oline le loro vittime.

I truffatori sono in grado di creare **falsi siti web di rivenditori** che sono molto convincenti e sembrano veri, anche sui social media come Facebook. L'indizio più grande che indica che un sito di vendita al dettaglio è una truffa è il metodo di pagamento - fate attenzione se vi viene chiesto di pagare tramite vaglia postale o altri metodi insoliti.

Una truffa di aste online si verifica quando un truffatore che vi dice che avete una seconda possibilità di acquistare un oggetto per cui avete fatto un'offerta dato che il vincitore si è ritirato. Il truffatore vi chiederà di pagare al di fuori della struttura di pagamento sicuro del sito di aste; se lo fate, perderete i soldi, non otterrete ciò per cui avete pagato e il sito di aste non sarà in grado di aiutarvi.

La **truffa di annunci online** è una truffa comune rivolta sia agli acquirenti che ai venditori. Gli acquirenti dovrebbero fare attenzione ai truffatori che pubblicano annunci falsi su siti web di annunci legittimi. Gli annunci pubblicitari possono riguardare

qualsiasi cosa, dalle case in affitto agli animali domestici, alle auto usate o alle macchine fotografiche, spesso a basso costo. Se mostrate interesse per l'articolo, il truffatore vi dice che sta viaggiando o si sta trasferendo all'estero e che un agente consegnerà la merce dopo aver ricevuto il pagamento. A seguito del pagamento non riceverete alcuna merce, né sarà possibile contattare il venditore.

Per i venditori, uno truffatore risponderà al vostro annuncio con un'offerta generosa. Se lo accettate, il truffatore pagherà con assegno o vaglia postale. Tuttavia, l'importo che riceverete è ben superiore al prezzo concordato. In questa **truffa in eccesso**, il "compratore" potrebbe dirvi che si è trattato di un errore e vi chiederà di rimborsare l'importo in eccesso tramite vaglia postale. Il truffatore spera che voi trasferiate i soldi prima di scoprire che il loro assegno è stato rimbalzato o che il vaglia postale è falso. Perderete i soldi, così come l'oggetto che avete venduto se lo avete già inviato.

Proteggetevi

- Scoprite esattamente con chi avete a che fare. Se si tratta di un rivenditore australiano, si è in una posizione molto migliore per risolvere il problema se qualcosa va storto.
- Controllate se il venditore è rispettabile, ha condizioni di rimborso e servizi di gestione dei reclami.
- Evitate qualsiasi accordo che richieda il pagamento anticipato tramite vaglia postale, bonifico bancario, trasferimento internazionale di fondi, carta pre-caricata o valuta elettronica. È raro recuperare i soldi inviati in questo modo. Non inviate mai via email denaro o dati della carta di credito o del conto online a persone che non conoscete o di cui non vi fidate.
- Pagate solo tramite il metodo di pagamento sicuro del sito web - cercate un indirizzo web che inizi con "https" e il simbolo di lucchetto chiuso.
- Non accettate mai assegni o vaglia per pagamenti superiori a quanto concordato né inoltrate mai denaro per conto di un'altra persona.

Truffe che colpiscono computer e cellulari

Ricordatevi: tutto ciò che si connette a Internet è vulnerabile.

Come funziona la truffa

I truffatori di accesso remoto vi telefonano sostenendo che il vostro computer è stato infettato da un virus. Se seguite le loro istruzioni, darete loro l'accesso e il controllo del vostro computer dove potranno rubare informazioni o installare malware. Potrebbero anche cercare di convincervi ad acquistare il software "anti-virus", che solitamente è eccessivamente costoso e disponibile gratuitamente su Internet.

Malware è un termine per qualsiasi software dannoso che può essere installato sul vostro computer o su altri dispositivi e include virus, spyware, ransomware, trojan horse e keystroke logger.

Keystroke logger e spyware consentono ai truffatori di registrare esattamente ciò che digitate sulla tastiera per scoprire password e dati bancari o per accedere alle informazioni personali e inviarle ovunque desiderino. Una volta installati, i truffatori possono controllare la vostra posta elettronica e i vostri account dei social media e accedere a qualsiasi informazione sul dispositivo, incluse le password. Possono anche usare i vostri account per inviare ulteriori truffe ai vostri amici e familiari.

Il ransomware è un altro tipo di malware che cripta o blocca il vostro dispositivo per impedirvi di usarlo fino a quando non viene effettuato un pagamento per sbloccarlo. Il pagamento non garantisce che verrà sbloccato o che sarà privo di virus nascosti, che possono anche diffondersi e infettare altri computer o dispositivi in rete.

Il malware viene comunemente fornito via e-mail e può sembrare che provenga da fonti legittime, come il fornitore di servizi, un'agenzia governativa o persino la polizia che vuole emettere una sanzione. Non cliccate sul link, né aprite eventuali allegati di cui non siete assolutamente certi. Potreste effettivamente scaricare software dannoso. Queste truffe prendono di mira sia le persone che le imprese.

Proteggetevi

- Diffidate dei download gratuiti che offrono musica, giochi, film e accesso a siti per adulti. Possono installare programmi dannosi a vostra insaputa.
- Tenete al sicuro reti d'ufficio, computer e cellulari. Aggiornate il software di sicurezza, cambiate le password e fate regolarmente il backup dei vostri dati. Archiviate i backup offsite e offline. www.staysmartonline.gov.au spiega come eseguire il backup dei dati e proteggere i cellulari.
- Non aprite allegati e non cliccate sui link nelle e-mail o nei messaggi dei social media ricevuti da estranei – premete semplicemente 'cancella'.

Furto d'identità

Tutte le truffe hanno il potenziale di rubarvi l' identità. Proteggersi dalle truffe significa anche mantenere al sicuro le informazioni personali.

Il furto d'identità è una minaccia in ogni truffa

La maggior parte delle persone associa le truffe al tentativo di rubarvi soldi. Tuttavia, anche le vostre informazioni personali sono preziose per i truffatori. I truffatori rubano i vostri dati personali per compiere attività fraudolente come fare acquisti non autorizzati con la vostra carta di credito, o usano la vostra identità per aprire conti bancari o telefonici. Potrebbero stipulare prestiti o svolgere altri affari illegali sotto vostro nome. Potrebbero persino vendere le vostre informazioni ad altri truffatori per ulteriori usi illeciti.

Il furto della vostra identità può essere sia finanziariamente che psicologicamente devastante. Possono essere necessari mesi per reclamare la vostra identità e le ripercussioni di questo furto possono durare anni.

Phishing—un truffatore vi contatta improvvisamente via email, telefono, Facebook o messaggio di testo e finge di provenire da un'azienda legittima come una banca, una compagnia telefonica o un provider di servizi Internet. Vi indirizza a una versione contraffatta del sito web dell'azienda che richiede i vostri dati personali per verificare i dati dei clienti a causa di un errore tecnico. Possono chiamare e fingersi rivenditori di beni di lusso sostenendo che qualcuno sta cercando di utilizzare la vostra carta di credito. Vi consigliano di contattare il vostro istituto bancario ma non riattaccano e rimangono in linea. Quando provate a

chiamare la banca, state ancora parlando con i truffatori che simulano una vera chiamata, imitano il personale della banca e chiedono il vostro conto bancario e i dati di sicurezza. In entrambi i casi, il truffatore acquisisce tutte le informazioni che gli vengono fornite e le utilizza poi per accedere ai vostri conti.

Sondaggi falsi—i truffatori offrono premi o ricompense come buoni regalo a rivenditori noti in cambio del completamento di un sondaggio online. Il sondaggio richiede di rispondere a una serie di domande, tra cui la divulgazione di importanti dati di identificazione o di coordinate bancarie.

ome parte di ogni truffa—i truffatori spesso richiedono informazioni personali in altre truffe. In una truffa di lotteria, i truffatori chiedono spesso la patente di guida o il passaporto per "provare la vostra identità prima che possano rilasciare il premio in denaro". Nelle truffe di incontri romantici potrebbero chiedere informazioni "per sponsorizzare la loro domanda di visto per venire a trovarvi in Australia".

Ricordatevi: fornire informazioni personali a un truffatore può essere altrettanto dannoso quanto regalare denaro. Non divulgate i vostri dati personali e teneteli al sicuro.

Proteggetevi

- **TPensate due volte a ciò che dite e fate online**
  Fate attenzione a condividere informazioni personali online, inclusi social media, blog e altri forum in rete. Fermatevi e riflettete prima di compilare sondaggi, partecipare a concorsi, cliccare su link o allegati, o anche "fare amicizia", "mettere Mi piace" o "condividere" qualcosa online.
- **Attenzione alle richieste di informazioni o denaro**
  I truffatori cercheranno di indurvi a consegnare i vostri dati utilizzando i nomi di aziende ben note o dipartimenti governativi. Se pensate che si tratti di una truffa, non rispondete. Utilizzate la rubrica o una ricerca online per verificare i dati di contatto dell'organizzazione. Non utilizzate mai i dati di contatto forniti nella richiesta originale.

Se avete fornito informazioni personali di identificazione ai truffatori, contattate ID ARE al numero 1300 432 273.

Truffe di lavoro e occupazione

Grande reddito - garantito?
Improbabile!

Come funziona la truffa

Le truffe di lavoro e occupazione riguardano offerte di lavoro a domicilio o da impostare e investire in "opportunità di affari". I truffatori promettono un lavoro, un alto stipendio o un grande ritorno sugli investimenti dopo i pagamenti iniziali. Questi pagamenti possono riguardare un "piano di business", corsi di formazione, software, uniformi, nullaosta di sicurezza, tasse o commissioni. Se pagate la commissione potreste non ricevere nulla o non quello che vi aspettavate o che vi era stato promesso.

Alcune offerte di lavoro possono essere una copertura per attività **illecite di riciclaggio di denaro,** dove vi viene chiesto di agire come un "account manager" o "assistente personale", ricevere pagamenti sul vostro conto bancario in cambio di una commissione e poi trasferire il denaro a un'azienda all'estero. Le truffe di lavoro vengono spesso promosse tramite e-mail di spam o pubblicità in annunci ben noti e su siti web di ricerca di lavoro - anche siti web di ricerca di lavoro del governo.

Un grosso pericolo con queste truffe di lavoro è che vi possono richiedere molti dettagli personali che non dovreste fornire, incluso il numero del vostro codice fiscale e le copie di passaporto o patente di guida. Queste informazioni potrebbero essere utilizzate in seguito per rubarvi l'identità.

Proteggetevi

- Attenzione alle offerte o ai sistemi che pretendono di garantire reddito o richiedere pagamenti in anticipo.
- Non acconsentite mai a trasferire denaro per qualcun altro - si tratta di riciclaggio di denaro sporco ed è illegale.
- Non fornite il numero di codice fiscale, la patente di guida o il passaporto quando fate domanda per un posto di lavoro. Potrebbe essere necessario fornire queste informazioni, ma solo dopo aver iniziato a lavorare.

Il riciclaggio di denaro è un reato: non accettate di trasferire denaro per conto di uno sconosciuto.

Truffe mediche e di beneficenza

I truffatori sono senza cuore e possono colpire durante la disperazione di alcuni periodi.

Come funziona la truffa

I truffatori approfittano delle persone che cercano di donare a una buona causa o di trovare una risposta a un problema di salute.

Le truffe di beneficenza coinvolgono truffatori che raccolgono denaro fingendo di lavorare per una causa legittima o per beneficenza, o per un'organizzazione fittizia da loro creata. Spesso i truffatori sfrutteranno un recente disastro naturale o una crisi che è stata riportata nelle notizie.

Queste truffe sottraggono donazioni necessarie alle organizzazioni di beneficenza legittime. Gli enti di beneficenza devono essere registrati presso il governo - donate con sicurezza ma controllate prima la loro registrazione.

Le truffe di miracoli offrono una gamma di prodotti e servizi che possono sembrare legittimi farmaci alternativi, che solitamente promettono rimedi rapidi ed efficaci per gravi condizioni mediche. I trattamenti sono spesso promossi usando false testimonianze di persone che sono "guarite".

Le truffe per la perdita di peso promettono una perdita di peso notevole con uno sforzo minimo o nullo. Questo tipo di truffa può comportare una dieta insolita o restrittiva, un esercizio fisico rivoluzionario, un dispositivo "che elimina i grassi", pillole innovative, cerotti o creme. Potrebbero richiedervi di effettuare un ingente pagamento anticipato o stipulare un contratto a lungo termine per ricevere prodotti di continuo.

Le false farmacie online offrono farmaci e medicine contraffatti a prezzi molto economici, talvolta senza la prescrizione medica. Questi farmaci possono avere ingredienti attivi limitati o assenti, con potenziali conseguenze letali per gli utenti.

Proteggetevi

- Se venite contattati da un venditore di beneficenza, chiedete loro di mostrarvi il documento di identificazione. Se avete dei dubbi su chi sono, non pagate.
- Controllate l'elenco delle associazioni di beneficenza senza scopo di lucro registrate presso l'associazione di beneficenza australiana.
- Rivolgetevi al vostro medico se state pensando di assumere medicinali, integratori o altri trattamenti "miracolosi" o con "risultati immediati".
- Chiedetevi: se questa è davvero una cura miracolosa, il vostro medico non ve l'avrebbe detto?

Truffe commerciali

I truffatori sfruttano il fatto che molte aziende sono indaffarate per ingannarle.

Come funziona la truffa

Le truffe rivolte alle aziende sono di ogni genere e rischiano di colpire nei periodi di maggiore lavoro, come ad esempio alla fine dell'anno finanziario.

Una **truffa di falsa fattura** è il trucco più diffuso utilizzato dai truffatori contro le aziende. I truffatori emettono fatture false per bollette, pubblicità, prodotti o servizi indesiderati o non autorizzati. La truffa della **business directory** è un esempio ben noto, in cui si riceve una fattura per un elenco presumibilmente noto. I truffatori vi ingannano per farvi iscrivere mascherando l'offerta come una fattura in sospeso o un elenco gratuito, ma con un'iscrizione nascosta nelle clausole del contratto.

La **truffa del nome di dominio** è un altro stratagemma usato dai truffatori, in cui si è ingannati ad iscriversi a una registrazione di dominio internet non sollecitata e molto simile alla propria. Potreste anche ricevere un falso avviso di rinnovo per il vostro nome di dominio effettivo e pagare senza accorgervene.

Una **truffa di forniture per ufficio** comporta l'accettazione e l'addebito per prodotti che non avete ordinato. Queste truffe comprendono spesso prodotti o servizi ordinati regolarmente come articoli di cancelleria e prodotti per la pulizia. I truffatori chiamano solitamente la vostra azienda e fanno finta che un servizio o un prodotto sia già stato ordinato.

Le truffe di reindirizzamento dei pagamenti coinvolgono un truffatore che utilizza le informazioni ottenute hackerando i sistemi del vostro computer. Si presentano come uno dei vostri fornitori abituali e vi dicono che i loro dati bancari sono cambiati. Potrebbero dirvi che hanno recentemente cambiato banca e potrebbero usare carta intestata e marchio copiati per convincervi della loro legittimità. Vi forniranno un nuovo numero di conto bancario e chiederanno che tutti i pagamenti futuri vengano effettuati di conseguenza. La truffa viene spesso scoperta solo quando il vostro fornitore regolare chiede il motivo per cui non é stato pagato.

Il ransomware può essere estremamente dannoso per qualsiasi azienda. La migliore difesa è quella di eseguire regolarmente il backup dei dati e archiviare i backup offsite e offline. V. maggiori informazioni a pagina 17.

Proteggetevi

- Non accettate offerte o affari immediatamente - richiedete sempre un'offerta scritta e chiedete consulenza indipendente se l'affare comporta denaro, tempo o un impegno a lungo termine.
- Non fornite mai i dati bancari, finanziari e contabili della vostra azienda a qualcuno che vi contatta inaspettatamente, che non conoscete e di cui non vi fidate.
- Le procedure di gestione efficaci possono essere davvero utili per prevenire le truffe: sono procedure chiaramente definite per la verifica e il pagamento di conti e fatture ed esaminano con molta attenzione le richieste di modifica dei dati bancari.
- Formate il vostro personale a riconoscere le truffe.
- Eseguite il backup dei dati aziendali offsite e offline.
- Fate attenzione alle e-mail che richiedono modifiche ai dati di pagamento. Verificate sempre le modifiche ai dati di pagamento direttamente con l'azienda o con la singola persona.

Come funzionano le truffe—l'anatomia di una truffa

La maggior parte delle truffe segue lo stesso schema e una volta capito, i trucchi del truffatore diventano più facili da individuare.

Se osservate attentamente tutti i diversi tipi di truffe descritti in questa pubblicazione, noterete subito che la maggior parte delle truffe si compone di tre fasi: (1) approccio; (2) comunicazione e (3) pagamento.

omprendere le parti di base di una truffa vi aiuterà a evitare l'attuale serie di truffe e a stare in guardia contro le nuove truffe che emergeranno in futuro.

1. L'approccio: metodo di consegna

Quando i truffatori vi contattano, presenteranno sempre una storia creata per farvi credere a una bugia. Il truffatore farà finta di essere qualcuno che non è, un funzionario governativo, un investitore esperto, un funzionario della lotteria o anche un ammiratore.

Per dirvi queste bugie, i truffatori useranno una serie di metodi di comunicazione.

Online

I truffatori si nascondono nell'ambiente anonimo di internet.

Le e-mail sono il metodo preferito per tentare una truffa dato che si tratta di un modo economico e semplice per comunicare su larga scala. Le e-mail di phishing che "pescano" le vostre informazioni personali sono il tipo di truffa elettronica più comune.

Piattaforme di social networking, siti di incontri e forum online consentono ai truffatori di "fare amicizia" con voi ed entrare nella vostra vita privata per accedere ai vostri i dati personali, i quali possono essere utilizzati contro di voi, i vostri familiari e amici.

Acquisti online, annunci e siti di aste vengono utilizzati dai truffatori per prendere di mira acquirenti e venditori, con il contatto iniziale spesso effettuato attraverso siti affidabili e di fiducia o siti web fasulli che sembrano reali. ercate opzioni di pagamento sicure e fate attenzione a metodi di pagamento insoliti come vaglia postale, Bitcoin o carte prepagate. Solitamente le carte di credito offrono una certa protezione.

Per telefono

Truffe telefoniche e anche SMS.

Le telefonate vengono fatte da truffatori ad abitazioni e aziende per una vasta gamma di truffe, da truffe fiscali minacciose a offerte di premi o “aiuto” con virus informatici. La disponibilità di chiamate telefoniche VOIP (Voice Over Internet Protocol) a buon mercato significa che i call center possono operare dall’estero con numeri di telefono che sembrano numeri locali. L’identificazione di colui che chiama può essere facilmente mascherata ed è uno dei tanti trucchi che i truffatori usano per farvi credere che sono qualcun altro.

I messaggi di testo SMS vengono utilizzati dai truffatori per inviare una vasta gamma di truffe, tra cui le truffe per competizioni o premi. In caso di risposta, è possibile che vi venga addebitato un costo aggiuntivo o che vi trovate registrati a un servizio di abbonamento. È più sicuro non rispondere né cliccare sui link nei messaggi di testo a meno che non si sappia da chi provengono. Possono anche contenere allegati o link a software dannosi sotto forma di foto, canzoni, giochi o app.

A domicilio

Attenzione - alcuni truffatori arriveranno direttamente sulla vostra porta per cercare di ingannarvi.

Le truffe porta a porta di solito coinvolgono il truffatore che promuove beni o servizi non consegnati o di pessima qualità. Potreste persino ricevere la fattura per un lavoro che non volevate o che non avete accettato. Una comune truffa porta a porta viene effettuata da commercianti loschi che si spostano da un posto all'altro e fanno riparazioni domestiche scadenti o semplicemente prendono i soldi e scappano.

Le aziende legittime possono vendere porta a porta, ma devono chiaramente identificare se stessi e la loro azienda e seguire altre regole. Avete diritti specifici quando si tratta di pratiche di vendita porta a porta, inclusa la possibilità di cambiare idea: per maggiori informazioni www.accc.gov.au/doortodoor.

I truffatori possono **fingersi** impiegati **di organizzazioni di beneficenza** per raccogliere donazioni. Approfitteranno di eventi recenti come inondazioni e incendi. Prima di fare una donazione, chiedete l'identificazione e controllate il loro libretto ufficiale di ricevute.

La posta viene ancora utilizzata per inviare **truffe per lotteria e giochi a premi, opportunità di investimento, truffe nigeriane** e **lettere di eredità false**. Un depliant lucido non garantisce che si tratti di un'offerta legittima.

Indipendentemente dal metodo di consegna utilizzato, la loro storia è sempre l'esca e se si abbocca, il truffatore tenterà di passare alla fase successiva.

2. Comunicazione e adescamento

Se date loro la possibilità di parlarvi inizieranno a usare tutti i loro trucchi per convincervi a separarvi dai vostri soldi.

Gli strumenti dei truffatori possono consistere di quanto segue:

- I truffatori creano **storie** elaborate, tuttavia **convincenti** per ottenere quello che vogliono.
- Usano i vostri **dati personali** per farvi credere di aver trattato con loro in precedenza e far sembrar lecita la truffa.
- I truffatori possono **contattarvi regolarmente** per creare fiducia e convincervi che sono amici, partner o interessi romantici.
- **Giocano con i vostri sentimenti** sfruttando l'entusiasmo per una vincita, la promessa di un amore eterno, l'empatia per uno sfortunato incidente, il senso di colpa per non aver aiutato o l'ansia e la paura dell'arresto o di una multa.
- I truffatori amano creare un **senso di urgenza** in modo da non avere il tempo di riflettere e reagire alle emozioni piuttosto che alla logica.
- Allo stesso modo, usano **tattiche di vendita ad alta pressione** dicendo che si tratta di un'offerta limitata, che i prezzi aumenteranno o che il mercato cambierà e perderete l'opportunità.
- Una truffa può avere tutti i tratti distintivi di un vero affare tramite l'utilizzo di **depliant lucidi** con gergo tecnico industriale supportati da uffici frontali, call center e siti web professionali.
- Con l'accesso a Internet e al software intelligente, è facile per i truffatori creare **documenti contraffatti e dall'aspetto ufficiale**. Un documento che sembra avere l'approvazione del governo o è pieno di termini legali può dare ad una truffa un'aria di autorità.

Gli strumenti dei truffatori sono progettati per farvi abbassare le difese, credere alla storia e agire rapidamente o irrazionalmente e procedere alla fase finale: la spedizione di denaro.

3. Invio di denaro

A volte il più grande indizio che vi fa capire che si tratta di una truffa è il modo in cui il truffatore vi chiede di pagare.

La richiesta di denaro può giungere a pochi minuti dalla truffa o dopo mesi di adescamento accurato. I truffatori hanno le loro preferenze su come dovete spedir loro i soldi.

I truffatori sono noti per indirizzare le vittime verso la loro sede di **rimessa di denaro** più vicina (ufficio postale, vaglia postale o persino la banca) per farsi inviare denaro. Sono noti per rimanere al telefono, dare istruzioni specifiche e possono persino inviare un taxi per i loro fini. Sono disposti ad accettare denaro con qualsiasi mezzo e questo può includere **bonifici bancari diretti, carte di debito prepagate, carte regalo, carte Google Play, Steam o iTunes** o valuta virtuale come **Bitcoin**. Qualsiasi richiesta di pagamento con un metodo insolito è un segnale di allarme che ci indica che si tratta di una truffa.

Di solito le carte di credito offrono una certa protezione e dovreste anche cercare opzioni di pagamento sicure dove "https" appare nell'indirizzo web e il sito ha il simbolo di un lucchetto chiuso.

Non inviate denaro a qualcuno che avete conosciuto solo online o al telefono, specialmente se si trova all'estero.

Siate consapevoli del fatto che i truffatori possono anche chiedere il pagamento sotto forma di merci di valore e regali costosi come gioielli od oggetti elettronici. Pagare denaro ai truffatori non è l'unica cosa di cui dovreste preoccuparvi: se aiutate a trasferire denaro per conto di uno sconosciuto, potreste involontariamente essere coinvolto in attività **illegali di riciclaggio di denaro**.

Le regole d'oro per proteggersi

State attenti alle truffe. Quando si ha a che fare con contatti non sollecitati di persone o aziende, sia per telefono, per posta, e-mail, di persona o su un sito di social network, considerate sempre la possibilità che l'approccio possa essere una truffa. Ricordatevi, se sembra troppo bello per essere vero, probabilmente lo è.

Scoprite con chi avete a che fare. Se avete soltanto conosciuto qualcuno online o non siete sicuri della legittimità di un'azienda, prendetevi del tempo per fare ulteriori ricerche. Fate una ricerca di immagini Google o su Internet e cercate altre persone che potrebbero aver avuto a che fare con loro.

dINon aprite testi sospetti, finestre pop-up o e-mail: cancellateli. Se avete dubbi, verificate l'identità del contatto attraverso una fonte indipendente come una guida telefonica o una ricerca online. Non utilizzate i dati di contatto forniti nel messaggio che vi è stato inviato.

Mantenete i vostri dati personali al sicuro. Mettete un lucchetto sulla vostra casella di posta e stracciate le bollette e altri documenti importanti prima di gettarli. Tenete password e numeri di pin in un posto sicuro. Fate molta attenzione a quante informazioni personali condividete sui siti di social media. I truffatori possono usare le vostre informazioni e immagini per creare un'identità falsa o per prendervi di mira per una truffa.

Fate attenzione ai metodi di pagamento insoliti. I truffatori chiedono spesso il pagamento tramite bonifici, carte prepagate e persino Google Play, Steam, o carte iTunes e Bitcoin. Questo rivela quasi sempre che si tratta di una truffa.

Tenete al sicuro cellulari e computer. Proteggetevi sempre usando password, non condividete l'accesso con altri (anche remoto), aggiornate il software di sicurezza e fate il backup dei contenuti. Proteggete la vostra rete WiFi con una password ed evitate l'uso di computer pubblici o hotspot WiFi per accedere ai servizi bancari online o fornire informazioni personali.

Scegliete le vostre password con attenzione. Scegliete password difficili da indovinare per gli altri e aggiornatele regolarmente. Una password complessa dovrebbe includere una combinazione di lettere maiuscole e minuscole, numeri e simboli. Non utilizzate la stessa password per ogni account/profilo e non condividete le password con nessuno.

Fate attenzione alle richieste di dati o denaro. Non inviate mai denaro o fornite numeri di carta di credito, dettagli dell'account online o copie di documenti personali a persone che non conoscete o di cui non vi fidate. Non accettate di trasferire denaro o beni per qualcun altro: il riciclaggio di denaro è un reato.

Fate attenzione quando acquistate online. Fate attenzione alle offerte che sembrano troppo belle per essere vere e utilizzate sempre un servizio di acquisti online che conoscete e di cui vi fidate. Pensateci due volte prima di utilizzare le valute virtuali (come Bitcoin): non hanno le stesse protezioni degli altri metodi di transazione, il che significa che non potete recuperare i soldi una volta inviati.

Dove trovare aiuto o supporto

Se avete perso denaro per una truffa o avete dato i vostri dettagli personali a un truffatore, è improbabile che recupererete i soldi. Tuttavia, ci sono dei passi che potete intraprendere immediatamente per limitare il danno e proteggervi da ulteriori perdite.

ontattate la vostra banca o istituto di credito

Se avete inviato denaro o informazioni bancarie personali a un truffatore, contattate immediatamente la vostra banca o istituto di credito. Potrebbero essere in grado di interrompere il trasferimento di denaro, controllare o chiudere il conto se il truffatore ha i vostri dati. Il fornitore della vostra carta di credito potrebbe essere in grado di eseguire un "charge back" (riaddebito) se la vostra carta di credito è stata fatturata fraudolentemente.

Recuperate l'identità rubata

Se sospettate di essere vittime di un furto d'identità, è importante agire rapidamente per ridurre il rischio di perdite finanziarie o altri danni.

ontattate **ID ARE**—un servizio gratuito finanziato dal governo che fornisce assistenza alle vittime di reati di identità. ID ARE può aiutarvi a sviluppare un piano di risposta per intraprendere le azioni appropriate per riparare i danni causati alla vostra reputazione, alla storia del credito e all'identità. Visitate il sito Web ID ARE all'indirizzo www.idcare.org o chiamate il numero 1300 432 273.

Richiedete il **certificato di vittima del ommonwealth**—il certificato vi aiuta a sostenere l'affermazione di essere stati vittime di un crimine di identità e può essere utilizzato per contribuire a ristabilire le vostre credenziali presso istituzioni governative o finanziarie. Visitate il Dipartimento del Procuratore Generale all'indirizzo www.ag.gov.au (o chiamate il numero 02 6141 6666) per saperne di più sulla protezione e il recupero della vostra identità.

ontattate un servizio di consulenza o supporto

Se voi o qualcuno che conoscete è stato truffato e potrebbe essere affetto da stress psicologico o depressione, rivolgetevi al vostro medico di famiglia, operatore sanitario locale o qualcuno di cui vi fidate. È inoltre possibile prendere in considerazione la possibilità di contattare servizi di consulenza o di supporto, quali:

Lifeline—quando avete bisogno di supporto in caso di crisi, contattate Lifeline al 13 1114 (24/7) o visitate www.lifeline.org.au

Beyondblue—per informazioni su depressione o ansia, contattate beyondblu al numero 1300 224 636 o visitate www.beyondblue.org.au

Assistenza telefonica per bambini (Kids Helpline)—servizi di consulenza e supporto online per giovani di età compresa tra 5 e 25 anni. ontatta il servizio di assistenza ai bambini al numero 1800 551 800 o visitate il sito www.kidshelpline.com.au

onsulenza finanziaria Australia (Financial ounselling Australia)—se avete difficoltà economiche chiamate il numero 1800 007 007 per parlare con un consulente finanziario gratuito o visitate il sito www.financialcounsellingaustralia.org.au.

Dove denunciare una truffa

Potete aiutare gli altri segnalando una truffa alle autorità competenti. Le vostre informazioni aiuteranno queste organizzazioni a costruire un quadro migliore delle ultime truffe e ad avvisare altre persone a cosa fare attenzione.

Le seguenti organizzazioni prendono segnalazioni su particolari tipi di truffe.

Scamwatch

Segnala le truffe all'A tramite Scamwatch - visitate www.scamwatch.gov.au

Precedete i truffatori

Precedete i truffatori: visitate il sito web di Scamwatch per conoscere le truffe indirizzate ai consumatori e alle piccole imprese australiane. Scoprite di più su come funzionano le truffe, come proteggervi e cosa fare se siete stati truffati.

Registratevi con il servizio di abbonamento Scamwatch per ricevere via email notifiche gratuite sulle nuove truffe in circolazione.

www.scamwatch.gov.au

Seguite Scamwatch su Twitter su @scamwatch_gov o su http://twitter.com/Scamwatch_gov

Se trovate una truffa su un sito web o una piattaforma di social media, segnalatela al sito in modo che possa essere esaminato e rimosso. Se i truffatori stanno impersonando un'organizzazione legittima come un dipartimento governativo o una banca, informateli in modo che possano avvisare gli altri.

Altre agenzie

Dovreste anche pensare di segnalare la vostra truffa ad altre agenzie che si occupano specificamente di determinati tipi di truffe.

Tipo di truffa	Agenzia
rimine informatico	Rete di segnalazione online dei cybercrimini australiani (A ORN) (Australian ybercrime Online Reporting Network) - visita www.acorn.gov.au
Truffe finanziarie e di investimento	Australian Securities and Investments ommission (ASI)—visitate www.moneysmart.gov.au o chiamate l'infoline ASI al 1300 300 630
Frode e furto	La vostra polizia locale - chiamate il 13 1444
Email spam e SMS	Autorità australiana per le comunicazioni e i media (A MA) - visitate www.acma.gov.au o chiamate il centro di assistenza clienti A MA al 1300 850 115
Truffe legate alle tasse	Ufficio imposte australiano (Australian Taxation Office) (ATO) - per segnalare una truffa fiscale o verificare se una persona che vi contatta da parte dell'ATO è legittima: • chiamate il numero 1800 008 540 o inoltrate la truffa delle vostre e-mail a ReportEmailFraud@ato.gov.au
Operazioni bancarie	La vostra banca o istituto finanziario

ontattate la vostra agenzia di protezione dei consumatori locale

Mentre l'A è l'agenzia nazionale che si occupa di questioni generali di tutela dei consumatori, le agenzie statali e territoriali potrebbero anche essere in grado di assistervi.

Australian apital Territory Office of Regulatory Services	www.accesscanberra.act.gov.au 13 2281
onsumer Affairs Victoria	www.consumer.vic.gov.au 1300 558 181
New South Wales Fair Trading	www.fairtrading.nsw.gov.au 13ww 3220
Northern Territory onsumer Affairs	www.consumeraffairs.nt.gov.au 1800 019 319
Queensland Office of Fair Trading	www.fairtrading.qld.gov.au 13 7468
South Australia onsumer and Business Services	www.cbs.sa.gov.au/ 13 1882
Tasmania onsumer, Building and Occupational Services	www.cbos.tas.gov.au/ 1300 654 499
Western Australia Department of Mines, Industry Regulation and Safety	www.consumerprotection.wa.gov.au/ 1300 304 054

Maggio informazioni

Il governo australiano dispone di risorse eccellenti per scoprire come stare sicuri online.

- Stay Smart Online Service—www.staysmartonline.gov.au
- CyberSmart website—www.cybersmart.gov.au
- Stay Smart Online guides—disponibili al sito www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au