I 10 migliori consigli per proteggersi dalle

Truffe di impersonificazione

Italian | Italiano

Australian Government | Be Connected Every Australian online.

Australian Government | National Anti-Scam Centre | SCAMWATCH

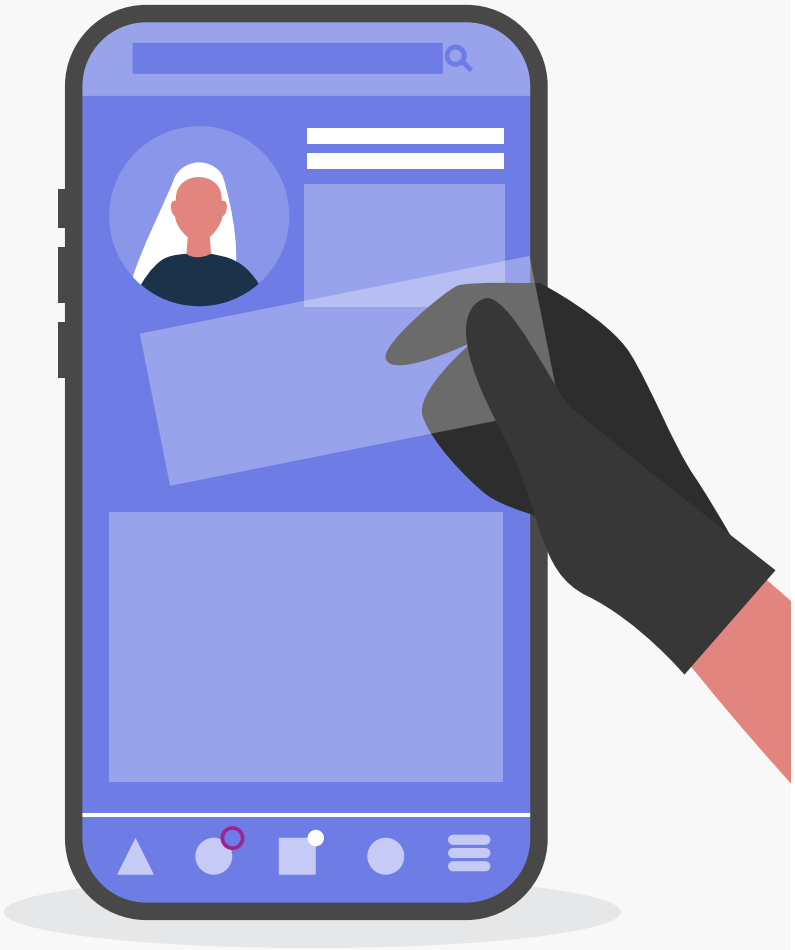
Le truffe stanno diventando sempre più sofisticate. In passato, gli errori di ortografia e grammatica le rendevano facilmente individuabili, ma le nuove tecnologie stanno rendendo le truffe sempre più difficili da scovare.

Il Centro Nazionale Anti-Truffa (National Anti-Scam Centre) ha unito le proprie forze con il governo, gli esperti del settore, le forze dell'ordine e le organizzazioni comunitarie per combattere le truffe. Anche tu puoi adottare delle misure per proteggerti. Una delle migliori misure di sicurezza è rimanere aggiornati sulle truffe nuove ed emergenti in modo da poterne riconoscere i segnali.

Questa guida, realizzata da Be Connected in collaborazione con Scamwatch, un'iniziativa del Centro Nazionale Anti-Truffa, ti aiuta a individuare le truffe di impersonificazione, ti spiega come proteggerti da esse e a chi rivolgerti per chiedere aiuto se ne diventi vittima.

Tutte le truffe riportate a titolo di esempio in questa guida sono reali.

In questa guida



Che cos'è una truffa di impersonificazione?

Nelle truffe di impersonificazione i criminali informatici fingono di essere organizzazioni legittime che conosci. Le comunicazioni sembrano provenire dalla tua banca, dal tuo fornitore di servizi internet, da un'agenzia governativa, da un rivenditore o persino da un amico o un familiare.

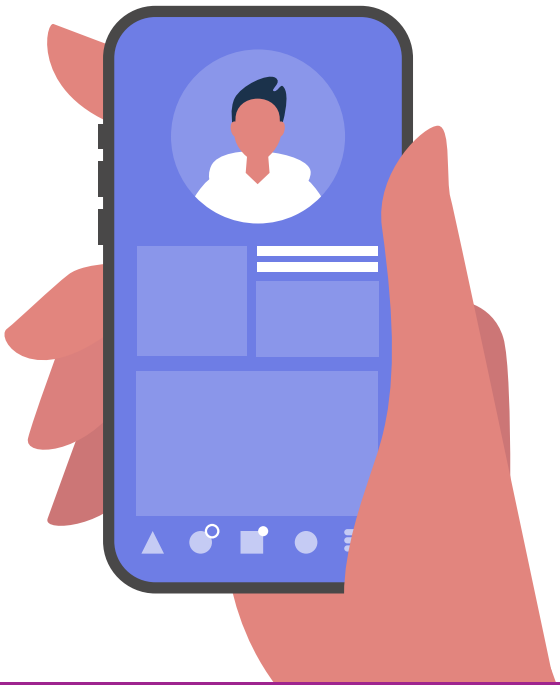
Fingendosi qualcuno di cui ti fidi, i truffatori creano un senso di urgenza per indurti a trasferire denaro o fornire informazioni personali, come password importanti, numeri di carte di credito o dati bancari.

I truffatori possono utilizzare diversi metodi per contattarti, tra cui messaggi di testo, telefonate, e-mail, post sui social media e siti web falsi che sembrano identici a quelli ufficiali.

Che cos'è lo spoofing?

I truffatori possono impersonare organizzazioni che conosci utilizzando la tecnologia, in modo che la loro chiamata o il loro messaggio sembrino provenire da una fonte attendibile. Questo fenomeno è noto come spoofing.

Fai dunque attenzione alle truffe e stai all'erta se ricevi comunicazioni inaspettate nelle quali ti vengono richieste informazioni personali, come ad esempio una password o qualsiasi tipo di pagamento. Contatta direttamente l'organizzazione da cui sembra provenire la richiesta per confermarne la veridicità.



Esistono diversi tipi di tecniche di spoofing, tra cui:

01. **Spoofing dell'ID chiamante:** i truffatori alterano le informazioni relative all'ID chiamante per mostrare un numero di telefono diverso da quello utilizzato in modo che la chiamata sembri provenire da un numero legittimo.

02. **Spoofing tramite SMS (o ID mittente alfanumerico):** i truffatori alterano il proprio numero di telefono per far sì che appaia come il nome di un'azienda (ad esempio, AusPost). Questo metodo può far apparire un messaggio di testo nella stessa conversazione o discussione contenente messaggi autentici provenienti da un'organizzazione.

03. **Spoofing tramite e-mail:** i truffatori alterano il loro indirizzo e-mail o il nome del mittente in modo che l'e-mail sembri provenire da una fonte attendibile. I truffatori possono falsificare il nome che visualizzi nel campo "Da" oppure l'indirizzo e-mail, spesso modificando o aggiungendo una lettera o un numero al nome di un dominio legittimo (ad esempio, @amaz0n.com anziché @amazon.com).

Truffe di impersonificazione comuni

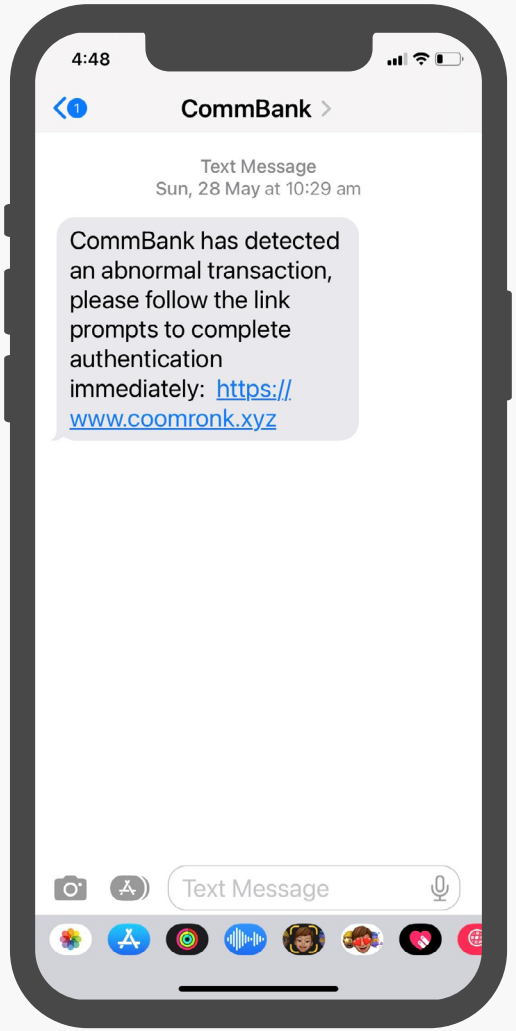
Truffe di impersonificazione riguardanti le banche

- Ricevi una chiamata o un messaggio di testo da qualcuno che dichiara di lavorare per il dipartimento di sicurezza della tua banca. L'interlocutore ti informa della presenza di una transazione sospetta, sostenendo che il tuo conto è stato violato. Ti esorta dunque a trasferire il tuo denaro su un altro conto così da "tenerlo al sicuro" o consentire l'effettuazione di "ulteriori indagini".
- Ricevi un messaggio di testo o un'e-mail che ti chiede di fare clic su un link per verificare i dettagli del tuo conto. Il collegamento ti porta a una pagina web falsa progettata per acquisire il tuo nome utente, password e altre informazioni personali.

Come faccio a sapere se si tratta di una truffa?

Sebbene la tua banca possa contattarti in caso di attività sospette sul tuo conto, non ti chiederà mai di trasferire denaro su un altro conto, né di condividere informazioni relative a un conto o dati personali, come per esempio password, PIN o codici di accesso monouso tramite un messaggio di testo, un'e-mail o una telefonata inaspettata.

I truffatori sono in grado di far apparire il loro numero di telefono come se fosse l'ID chiamante della tua banca, quindi non presumere automaticamente che il tuo interlocutore sia legittimo. I truffatori potrebbero anche conoscere alcune informazioni che ti riguardano, ma tutti i dettagli in loro possesso sono stati probabilmente ottenuti in modo fraudolento.



Esempio di truffa di impersonificazione mediante SMS bancario proveniente da un numero contraffatto che chiede di fare clic su un link per verificare i dati.

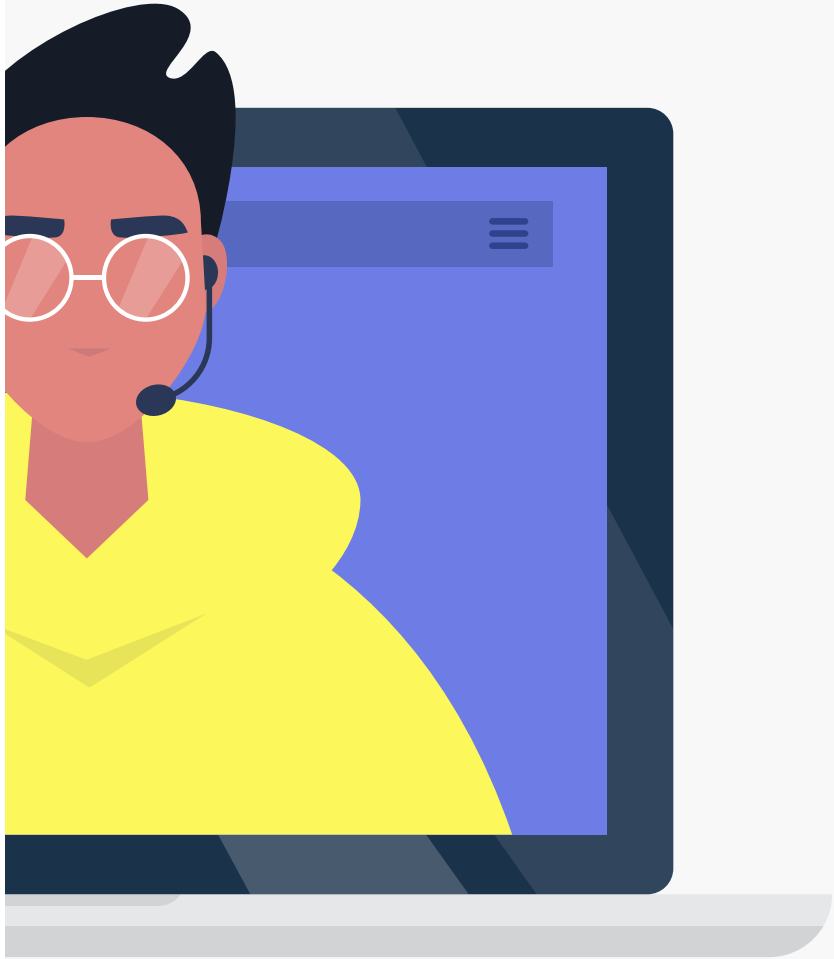
Truffe relative al supporto tecnico

- Un operatore che afferma di lavorare per un fornitore di servizi internet, una società di telecomunicazioni o di informatica ti chiama per informarti dell'esistenza di un problema con la tua connessione internet o con il tuo computer. L'operatore potrebbe comunicarti che il tuo computer è stato violato, ha un virus, sta funzionando lentamente o sta per essere disconnesso. A quel punto, ti fornirà indicazioni su come scaricare un'app o un software per consentirgli di accedere al tuo computer da remoto e poterlo "riparare".
- Sullo schermo del computer appare un messaggio di avviso che ti invita a chiamare immediatamente il numero di telefono indicato per ricevere assistenza riguardo a un problema rilevato.

Come faccio a sapere se si tratta di una truffa?

Le aziende che operano in maniera legittima non ti chiameranno mai per comunicarti l'esistenza di un problema con la tua connessione internet o con il tuo computer, ma si aspettano che sia tu a contattarli in caso di problemi. Non ti chiederanno mai di scaricare alcun tipo di software o app che consenta loro di accedere al tuo dispositivo.

Chiudi i messaggi pop-up sospetti facendo clic sulla "x" che si trova nell'angolo in alto a destra della casella. Se questo non funziona, prova a fare clic all'esterno della casella o a chiudere la pagina web in cui appare. Se la casella di pop-up continua ad apparire sullo schermo, prova a tenere premuti i tasti ALT e F4 sul tuo computer Windows per chiudere il browser web. Su un computer Apple, seleziona l'opzione "Uscita forzata" dal menu Apple e poi il browser che desideri chiudere.



Truffe relative alla sospensione di un account

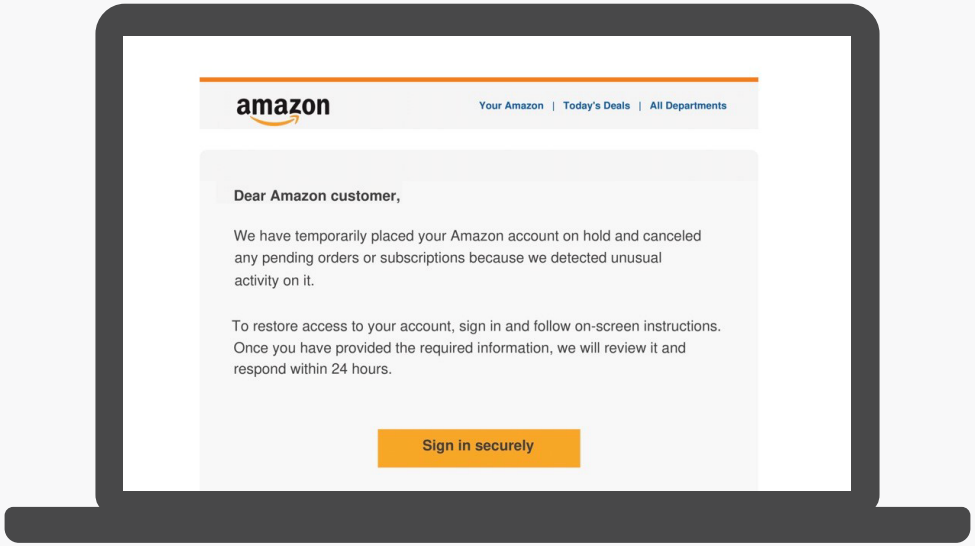
Un'e-mail o un messaggio di testo che sembra provenire da un'organizzazione che conosci, come Amazon, PayPal o Netflix, ti informa che il tuo account è stato sospeso a causa di attività sospette e che devi fare clic su un link per confermare la tua identità.

I truffatori utilizzano tattiche intimidatorie per indirizzarti verso un sito web falso che acquisisce dati personali come il tuo nome utente, password e dati bancari o della carta di credito.

Come faccio a sapere se si tratta di una truffa?

Amazon, PayPal e Netflix non ti chiederanno mai di condividere informazioni personali come password, dati bancari o delle carte di credito tramite un link contenuto in un'e-mail o in un messaggio di testo che non ti aspettavi di ricevere. Sebbene diverse organizzazioni adottino approcci differenti nel contattare i clienti, è sempre meglio andare sul sicuro e trattare questo tipo di e-mail, SMS o chiamate con cautela.

In caso di dubbi sull'effettiva provenienza di un messaggio, contatta direttamente l'azienda in questione cercando i suoi contatti online. Non utilizzare mai i contatti forniti nel messaggio di testo, nell'e-mail o durante la telefonata.



Esempio di un'e-mail fraudolenta che sembra provenire da Amazon e che esorta a fare clic sul link per fornire informazioni personali.

Fai attenzione alle tattiche intimidatorie

I truffatori usano tattiche intimidatorie per creare un senso di urgenza e spingerti ad agire. Ecco alcune cose che potrebbero dire per attirare la tua attenzione:

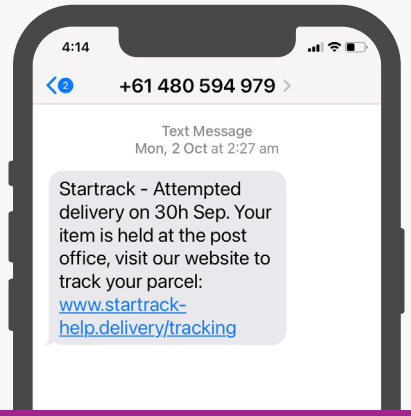
- Sono state rilevate attività insolite nel tuo account.
- Ci sono stati tentativi di accesso non autorizzati.
- Il tuo account è bloccato/sospeso.
- Il tuo pagamento è stato rifiutato.
- Non siamo stati in grado di convalidare i tuoi dati di fatturazione.

Truffe relative a tentativi di consegna non riusciti

Un'e-mail o un messaggio di testo che sembra provenire da Australia Post o da un corriere come FedEx ti informa che c'è un problema o un ritardo con la consegna di un tuo ordine. Per poter ricevere il pacco, ti chiede di pagare un costo di spedizione oppure di "aggiornare i tuoi dati".

Come faccio a sapere se si tratta di una truffa?

Australia Post, FedEx e altre compagnie di spedizioni legittime non richiedono mai informazioni personali o pagamenti tramite messaggi di testo, e-mail o chiamate. Se sei in attesa di una consegna, è meglio effettuare il tracciamento tramite l'app sicura o il servizio di tracciamento online il cui link è contenuto nell'e-mail di conferma dell'ordine. Se non sei in possesso di queste informazioni, chiama direttamente il corriere per conoscere lo stato del tuo pacco.



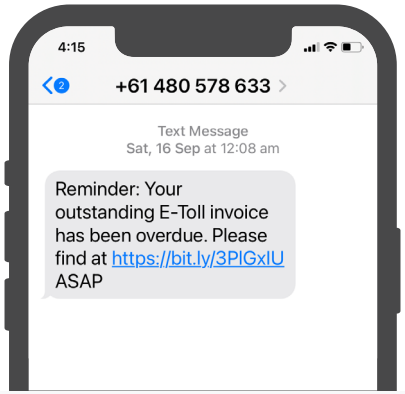
Esempio di un messaggio di testo che sembra provenire da un corriere.

Truffe relative ai pedaggi stradali

Un messaggio proveniente da un operatore di pedaggi stradali ti informa che hai un pagamento in arretrato. Il messaggio ti invita ad agire immediatamente per evitare di dover pagare una multa e include un link per effettuare il pagamento. Questo link però ti conduce a un sito web falso progettato per rubare i tuoi dati finanziari.

Come faccio a sapere se si tratta di una truffa?

Se hai ricevuto un messaggio che ti avvisa che il tuo account collegato ai pedaggi stradali è scaduto o ha fondi insufficienti, potrebbe trattarsi di una truffa. Visita il sito web o l'app del gestore dei pedaggi stradali per accedere al tuo account e verificare le tue attività più recenti.



Esempio di truffa mediante un SMS relativo ai pedaggi stradali.

Truffe relative a investimenti falsi

Vedi un'incredibile opportunità di investimento che sembra essere approvata da una celebrità o da un influencer finanziario e che promette un rendimento elevato garantito con rischi minimi o nulli. Dopo aver richiesto maggiori informazioni, ti viene fornito il link a un sito web dall'aspetto professionale e ricevi materiale promozionale sofisticato.

Come faccio a sapere se si tratta di una truffa?

Se un'offerta sembra troppo vantaggiosa per essere vera, probabilmente è una truffa. I truffatori utilizzano tattiche per fare pressione e convincerti ad agire rapidamente in modo da non lasciarti "sfuggire" l'occasione. Fai attenzione a e-mail, siti web o annunci riportanti testimonianze e promesse esagerate di rendimenti elevati.

Il "consulente" che ti sta aiutando potrebbe affermare di non aver bisogno di una licenza per offrire servizi finanziari in Australia (Australian financial services, AFS). Se te ne fornisce una, controlla sempre che la persona con cui hai a che fare sia il vero titolare della licenza.

Truffe relative a siti web falsi

Vedi un annuncio su Facebook che pubblicizza la vendita di un noto marchio di barbecue per 100 dollari quando normalmente ha un prezzo di 900 dollari. Fai clic sul link al sito del rivenditore e ti accorgi che i pagamenti con carta di credito prevedono una commissione del 2,99%, quindi scegli di pagare tramite bonifico bancario così da ricevere un ulteriore sconto del 5%. Ricevi un'e-mail di conferma, ma nessun barbecue.

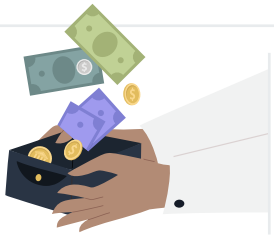
Come faccio a sapere se si tratta di una truffa?

I siti web fasulli offrono prezzi troppo bassi per essere veri, richiedono forme di pagamento insolite o presentano altri campanelli di allarme come un URL simile a quello di un negozio ufficiale (ad esempio, webberbbqs.com rispetto al sito internet legittimo weber.com).

I truffatori possono anche pubblicare annunci a pagamento sui social media e sui motori di ricerca come Google, noti come annunci sponsorizzati, quindi fai attenzione quando clicchi su questo tipo di pubblicità.

I 10 migliori consigli per proteggersi

01. Fai attenzione alle chiamate inaspettate. Lascia che le chiamate provenienti da numeri di telefono che non riconosci vengano trasferite alla segreteria telefonica.



02. In caso di comunicazioni inaspettate, fermati e rifletti prima di fornire dati personali o finanziari. Chiediti: potrebbe trattarsi di una truffa?

03. Fai attenzione alle e-mail che utilizzano tattiche intimidatorie. Controlla il nome visualizzato e l'indirizzo e-mail. Corrispondono? Ad esempio, il campo "Da" indica "Supporto Amazon", ma l'indirizzo e-mail è amazonsupport830@gmail.com

04. Non fidarti di un messaggio di testo solo perché appare nella stessa conversazione contenente messaggi di un'organizzazione che conosci. Potrebbe comunque essere una truffa.

05. In caso di dubbi riguardo a un messaggio o una chiamata che hai ricevuto, contatta l'organizzazione da cui sembra provenire. Puoi farlo tramite il suo sito web ufficiale o l'app sicura che hai scaricato sul tuo smartphone o tablet.

06. Non dare mai a nessuno per telefono la tua password, il PIN o il codice monouso, anche se il tuo interlocutore afferma di lavorare per la tua banca o per un'agenzia governativa e ti ha fornito informazioni sul tuo account.

07. Non cliccare mai sui link presenti nei messaggi di testo. Potrebbero anche essere innocui, ma è meglio andare sul sicuro. Lo stesso vale per gli allegati e i link contenuti nelle e-mail, a meno che tu non conosca con certezza l'identità del mittente.

08. Non seguire mai le istruzioni di una persona che ti chiama inaspettatamente e ti chiede di scaricare un'app o installare un software che le consente di accedere al tuo dispositivo. Riaggancia immediatamente.

09. Non accedere mai ai tuoi account online tramite un link riportato in un'e-mail o in un messaggio di testo. Inserisci invece l'URL dell'azienda nel browser o utilizza la loro app sicura per accedere al tuo account.

10. Prima di effettuare un pagamento online, controlla sempre l'URL del sito web (si tratta del sito ufficiale?) e verifica che non ci siano metodi di pagamento insoliti o informazioni incomplete o scritte in maniera inadeguata nelle sezioni "Chi siamo", "Spedizioni e resi" e in altre sezioni presenti nella parte inferiore del sito web.

In caso di dubbi, esegui una ricerca online inserendo il nome dell'organizzazione o del sito web in questione e la parola "truffa".

Pensi di aver subito una truffa?

A chi rivolgersi per ottenere aiuto

Essere vittima di una truffa può avere un forte impatto finanziario ed emotivo ed è dunque importante chiedere aiuto e agire rapidamente. Esistono diverse azioni che puoi intraprendere:

1. Contatta immediatamente la tua banca per impedire l'esecuzione di ulteriori transazioni.
2. Contatta IDCARE, un servizio di supporto gratuito per le persone che sono state colpite da truffe o furti di identità. Chiama il numero 1800 595 160 o visita idcare.org
3. Cambia immediatamente le tue password e assicurati che siano sicure.
4. Segnala la truffa a Scamwatch per avvisare gli altri: scamwatch.gov.au/report-a-scam
5. Richiedi assistenza. Se non ti senti a tuo agio a parlare con amici o familiari, contatta Lifeline o Beyond Blue per una conversazione privata. Se hai perso una somma considerevole di denaro, contatta la National Debt Helpline.

   Beyond Blue: 1300 22 4636 (24/7) oppure visita il sito beyondblue.org.au

   Lifeline: 13 11 14 (24/7) oppure visita il sito lifeline.org.au

   National Debt Helpline: 1800 007 007 (giorni feriali, dalle 9:30 alle 16:30) oppure visita il sito ndh.org.au

Per ulteriori informazioni

Fai clic sui riquadri sottostanti per saperne di più:

PODCAST

Evitare le truffe di impersonificazione

PODCAST

Informazioni che i truffatori online non vogliono tu sappia

ARGOMENTO

Identificare ed evitare le truffe

ARGOMENTO

Sicurezza online avanzata

ARTICOLO

Come bloccare le chiamate indesiderate

ARTICOLO

Furto di identità: che cos'è e come evitarlo

The Little Book of Scams (Il piccolo libro delle truffe) è uno strumento riconosciuto a livello internazionale che fornisce maggiori informazioni su diverse truffe comuni e su come proteggersi.

Visita il sito web di Scamwatch per ricevere aggiornamenti sulle ultime truffe e per ottenere consigli su come proteggerti.

Informazioni su Be Connected

Be Connected è un'iniziativa del Governo australiano volta a sviluppare le competenze digitali, la fiducia e la sicurezza online delle persone anziane australiane, tramite lezioni gratuite di informatica, brevi corsi online e molto altro ancora su vari argomenti. Il sito web e i contenuti didattici di Be Connected sono gestiti dall'eSafety Commissioner.

Informazioni su Scamwatch

Scamwatch è un'iniziativa gestita dal Centro Nazionale Anti-Truffa, istituita per rendere l'Australia un bersaglio più difficile per i truffatori. L'iniziativa ha l'obiettivo di sensibilizzare la comunità in materia di truffe, insegnando come riconoscerle, evitarle e segnalarle. Il centro condivide inoltre le informazioni provenienti dalle segnalazioni di truffe e collabora con il governo, le forze dell'ordine e il settore privato per contrastarle e prevenirle.