Stare al sicuro dalle truffe

La fiducia e la sicurezza sono di priorità assoluta a CommBank. Stiamo vedendo sempre più casi di clienti che vengono forzati o ingannati da truffatori ad inviare denaro. Queste truffe possono essere complesse e prendere varie forme. È importante tenere gli occhi aperti e avvertirci se c'è qualcosa di strano. Per maggiori informazioni su come proteggerti e notificare una truffa, dai un'occhiata a **commbank.com.au/safe**.

Autenticazione e verifica

- Completa il controllo di sicurezza sull'app di CommBank.
- Attiva l'autenticazione a più fattori, che aggiunge un controllo supplementare per confermare la tua identità.
- Utilizza **CallerCheck** per verificare l'identità delle chiamate che dicono di provenire dalla banca.
- Utilizza **CustomerCheck** in filiale per confermare la tua identità al personale.
- **NameCheck** ti avviserà se i dettagli del conto su un pagamento che effettui per la prima volta non sembrano corretti.

Sicurezza dei dispositivi e dei pagamenti

- Mantieni il software antivirus aggiornato e proteggi il tuo computer dalle comuni minacce.
- Utilizza metodi di pagamento sicuri cui il pagamento contactless o con l'inserimento della carta.
- Non condividere dispositivi che hanno accesso al tuo portafoglio digitale.

Password e dati personali

- Non condividere mai password o PIN e sii prudente quando condividi dati personali.
- Non fornire ma il tuo NetCode a nessuno, nemmeno al personale di CommBank.
- Puoi cambiare la password su NetBank e sull'app di CommBank in qualsiasi momento.
- Crea password complesse e cambiale regolarmente Per leggere i nostri consigli sulla creazione delle password, visita commbank.com.au/password-security.

Email, SMS e Online

- Non cliccare su link contenuti in email o SMS sospetti.
- Se non sei sicuro di un messaggio, rivolgiti a qualcuno di cui ti fidi o contatta l'organizzazione direttamente tramite i recapiti ufficiali.
- Riaggancia se ricevi telefonate automatiche, sospette o di minaccia da parte di terzi.
- Sii prudente se ti contattano persone che non conosci sui social media e sulle piattaforme online.

Fermati. Controlla. Rifiuta.

Fermati. Qualcosa sembra strano? Se hai dei dubbi, la miglior cosa da fare è fermarti. Fai un respiro.
Controlla. Chiedi a qualcuno di cui ti fidi o contatta l'organizzazione direttamente tramite i recapiti ufficiali.
Rifiuta. Riaggancia, elimina l'email, blocca il numero di telefono. Cambia le password.

Se pensi di essere vittima di una truffa, contatta CommBank immediatamente al numero **13 22 21**, oppure al numero **+61 2 9999 3283** dall'estero.

Se l'inglese non è la tua prima lingua, il servizio di traduzione e interpretariato gratuito del governo può aiutarti a comunicare con noi. Il servizio è disponibile in oltre 150 lingue. Possiamo richiedere questo servizio quando ci chiami o ti rechi in filiale.

Cose che dovresti sapere: Non ti invieremo mai un'email o un SMS in cui chiediamo i tuoi dati bancari come ad esempio il tuo NetBank Client ID, la tua password, oppure il tuo NetCode; né includeremo un link per effettuare l'accesso diretto da un'email oppure un SMS. Scrivi sempre commbank.com.au nel browser oppure utilizza l'app CommBank per accedere in modo sicuro ai servizi bancari. Se c'è qualcosa che sembra sospetto su CommBank, inoltralo a hoax@cba.com.au ed eliminalo. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL e Licenza australiana di credito n° 234945.

Commonwealth Bank

Pubblicato il 01/06/2024

Informazioni importanti sulle truffe comuni

Investimenti (tra cui Cripto)

I truffatori allettano le persone con la promessa di offrire alti introiti, che spesso includono cripto o altre opportunità di investimento. I truffatori possono cercare di contattarti per telefono, email o attraverso le piattaforme dei social media.

Consigli per proteggerti:

- Se è troppo bello per essere vero, probabilmente lo è.
- Sii prudente quanto ricevi offerte senza che tu le abbia chieste e quando qualcuno ti fa pressione affinché tu investa o faccia qualcosa velocemente.
- Verifica prima che la compagnia o il broker siano legittimi sul sito web di ASIC.

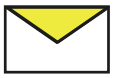
Accesso remoto

Quando un truffatore ti chiama e cerca di ottenere accesso ai tuoi account o al tuo dispositivo, fingendo di far parte di una compagnia o organizzazione fidata.

Consigli per proteggerti:

- Non scaricare mai software per l'accesso remoto su richiesta o sotto pressione di qualcuno che ti chiama.
- Puoi sempre richiamare l'organizzazione usando i suoi recapiti legittimi disponibili sul suo sito ufficiale.
- Se ricevi una chiamata da qualcuno che dice di essere di CommBank, puoi sempre chiederci di verificare la chiamata attraverso la funzione di controllo CallerCheck all'interno dell'app.

Email aziendale compromessa



I truffatori possono prendere di mira aziende con email ottenute da un indirizzo compromesso oppure email preparate in modo da sembrare che provengano da un contatto fidato come ad esempio: il tuo assistente, cliente, avvocato, manager o fornitore.

Consigli per proteggerti:

- Prima di effettuare pagamenti per la prima volta oppure cambiare dei dati di pagamento, prima chiama l'organizzazione sul suo numero di contatto ufficiale per confermare i dati.
- Utilizza la funzione NameCheck quando effettui pagamenti, per vedere se il nome dell'account corrisponde al BSB e al numero di account che ti sono stati forniti.
- Prepara i dipendenti a riconoscere e segnalare tentativi di phishing.

Phishing e Smishing

I truffatori utilizzano email oppure messaggi di testo ingannevoli che possono includere un link che ti porta su un sito fraudolento oppure che ti chiede dati personali sensibili.

Consigli per proteggerti:

- Non cliccare su link contenuti in email o SMS sospetti.
- Puoi confermare l'autenticità di un messaggio contattando l'organizzazione direttamente, utilizzando i suoi metodi di contatto ufficiali disponibili.
- Segnala eventuali messaggi sospetti da parte di CommBank a hoax@cba.com.au

Informazioni importanti sulle truffe comuni

Relazione

I truffatori creano profili falsi per intrecciare relazioni e manipolare le vittime affinché inviino denaro o dati personali.

Consigli per proteggerti:

- Non inviare mai denaro e non condividere mai password, i dati di carte di credito o di account con persone di cui non ti fidi.
- Cerca il tuo potenziale partner online oppure per mezzo di Google o sulle app di social media. Prova a cercare le immagini di quella persona per identificare se le foto che ti sono state inviate appartengono a qualcun altro.
- Parla della tua relazione online con familiari e amici. Potrebbero essere in grado di offrirti un punto di vista e identificare dei campanelli di allarme che tu potresti non avere notato.

Acquisti online

I truffatori creano negozi o pubblicità online per indurre gli acquirenti ad acquistare prodotti non esistenti o contraffatti.

Consigli per proteggerti:

- Effettua acquisti su siti web rispettabili e sicuri e diffida di offerte che sembrano troppo belle per essere vere.
- Utilizza metodi di pagamento sicuri ed evita di pagare i venditori con bonifici.
- Non avere fretta e non farti mettere fretta da “offerte limitate” o “conti alla rovescia” che indicano la fine della svendita.

Opportunità di impiego

Quando un’offerta di lavoro richiede poco o nessun sforzo a cambio di un guadagno ingente o promette guadagni veloci.

Consigli per proteggerti:

- Verifica la compagnia e l’offerta attraverso canali ufficiali ed effettua una ricerca sulla compagnia per assicurarti che sia legittima ed operativa.
- Diffida di offerte di lavoro attraverso i social media, chat crittografate, email, telefono o lettere ricevute da persone che non hai mai incontrato o compagnie che non conosci.
- Una compagnia legittima non ti chiederebbe mai un acconto o di utilizzare i tuo dati bancari personali per agevolare fondi aziendali o attività commerciali.

Minacce e sanzioni

I truffatori si spacciano per autorità od organizzazioni fidate per estorcere denaro attraverso la minaccia di una multa o di intraprendere un’azione legale.

Consigli per proteggerti:

- Riaggancia se qualcuno ti chiama e ti minaccia e contatta direttamente l’organizzazione.
- Un’organizzazione legittima non ti chiederà mai di pagare utilizzando metodi di pagamento insoliti come ad esempio buoni regalo o carte prepagate dei negozi, voucher iTunes, bonifici o Bitcoin.
- Se sei preoccupato per la tua sicurezza, contatta la linea di assistenza della polizia.