



AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

Attuali raggiri legati al COVID-19 (coronavirus)

Giugno 2020

Truffatori stanno sfruttando la pandemia del COVID-19 (coronavirus) per raggirare il pubblico in tutta l'Australia. Vi sono tre tipi principali di raggiri ai quali stiamo assistendo:

'Phishing' aventi per oggetto i vostri dati personali

Truffatori stanno chiamando o inviando mail e messaggi testuali fingendo di essere aziende e organi del governo e usando dati o servizi legati al COVID-19 per sollecitarvi a cliccare su link o a scaricare del software con l'intenzione di carpire i vostri dati personali (fenomeno definito 'phishing').

Raggiri aventi per oggetto i fondi pensione

Truffatori stanno approfittando di persone in difficili situazioni economiche a causa del COVID-19 tentando di rubare i loro fondi pensione o offrendo servizi superflui a fronte del pagamento di una tariffa.

Tali truffatori fingono di rappresentare un fondo pensione o un servizio finanziario nel tentativo di carpire informazioni relative ai vostri conti di fondo pensione ricorrendo ai seguenti stratagemmi:

- Offrendovi assistenza per prelevare fondi prima dei termini di legge.
- Garantendovi che non vi sarà negato l'accesso al vostro conto ai sensi delle regole relative al COVID-19.
- Controllando se il vostro conto ha diritto a ricevere vari benefici.

Raggiri aventi per oggetto lo shopping on-line

Truffatori hanno creato falsi punti di vendita su internet per vendere prodotti che non esistono — ad esempio, cure o vaccini per il COVID-19, e prodotti difficili da trovare quali le mascherine facciali.

Come potete proteggervi da questi raggiri

- Non dovete cliccare su hyperlink in messaggi testuali o dei social media o in mail, anche se sembrano provenire da una fonte fidata.
- Andate direttamente al sito tramite il vostro browser. Ad esempio, per raggiungere il sito MyGov, digitate voi stessi 'my.gov.au' nel browser.
- Non dovete mai rispondere a chiamate e messaggi non sollecitati con cui vi si chiede di fornire dati personali o finanziari, anche se sostengono di provenire da un'azienda o da un organo pubblico affidabile — premete "cancella" o riattaccate.
- Il modo migliore di smascherare un falso commerciante o un raggio nel campo dello shopping sui social media è di consultare varie recensioni prima di procedere all'acquisto. Al momento non esistono vaccini o cure per il COVID-19.
- Fate attenzione a venditori che richiedono metodi insoliti di pagamento, ad esempio pagamento anticipato tramite vaglia postali, bonifici bancari, bonifici internazionali, carte prepagate o divise elettroniche come Bitcoin.

RICORDATE Se nutrite qualsiasi dubbio,
non procedete.

Maggiori informazioni sui raggiri si trovano sul [sito Scamwatch](#), che comprende indicazioni su come [sporgere una denuncia](#) e [dove trovare assistenza](#).