Australian Banking Association

Tieniti al sicuro:
sii consapevole di truffe e frodi.

Le truffe e frodi aventi come tema il COVID-19 aumenteranno probabilmente nei prossimi mesi.

I truffatori usano email, telefonate o messaggi di testo fasulli per cercare di ottenere informazioni personali. Fanno finta di essere della tua banca, dell'Organizzazione mondiale della sanità, del governo, di enti caritatevoli o di legittime attività commerciali, come agenti di viaggio, fornitori di energia elettrica, di servizi telefonici o internet, o addetti del tuo supermercato locale.

Proteggiti

La tua banca non manderà MAI un'email o un messaggio di testo chiedendo dettagli su conti bancari o informazioni finanziarie, e ciò include le richieste di aggiornamento del tuo indirizzo o dei dettagli per il login per operazioni bancarie via telefono, via cellulare o via internet.

Il governo e altre organizzazioni legittime non ti chiederanno MAI di aggiornare i tuoi dettagli cliccando su di un link. Se sei in dubbio, parlane con un amico o un familiare, o contatta direttamente l'organizzazione interessata chiedendo delucidazioni.

Se ricevi una telefonata da qualcuno che non conosci che ti chiede informazioni personali, APPENDI. Chiama l'azienda direttamente e controlla se ha veramente chiamato.

Non aprire MAI allegati di persone od organizzazioni che non conosci. Diffida sempre di offerte che sembrano troppo belle per essere vere oppure presuppongono che tu dia troppe informazioni.

La tua banca può essere d'aiuto, contattala immediatamente se:

- Hai riferito i tuoi dettagli bancari in risposta a una telefonata, un'email o un messaggio di testo fasullo
- Hai accidentalmente cliccato su di un link o hai scaricato qualche allegato
- Hai notato transazioni insolite nei tuoi conti.

Come riconoscere una truffa

- Ti è stato chiesto di aggiornare o confermare dati personali, tra cui l'indirizzo, la data di nascita, i dettagli del conto bancario, il numero di codice fiscale, o qualunque PIN o password.
- L'email o il messaggio di testo contiene dei link che sembrano sospetti. Se non sei sicuro, chiedi aiuto a un familiare o a un amico.
- Ti è stato chiesto un pagamento immediato o un deposito anticipato.
- Se l'offerta è troppo buona per essere vera, probabilmente non lo è.
- L'indirizzo email non corrisponde a quello dell'azienda.
- Chi chiama chiede di avere accesso remoto al tu computer.

Australian Banking Association

www.ausbanking.org.au

Suggerimenti più importanti per proteggere le tue informazioni finanziarie da truffe e frodi

- Appendi quando ricevi telefonate sospette, vai piuttosto nel sito web dell'azienda o trova il suo numero e telefona direttamente.
- Non condividere mai le password o i PIN. Proteggi con una password le tue apparecchiature. Se usi un computer in condivisione con altri, non salvare mai le password e fai sempre il logout dal tuo conto.
- Controlla regolarmente i tuoi conti bancari in modo da notare velocemente transazioni sospette.
- Evita di strisciare la tua carta per fare acquisti. E' spesso più sicuro usare la modalità contactless e inserire la carta dentro il lettore.
- Blocca la possibilità di ottenere prelievi di contanti dalle carte di credito.
- Parla alla tua banca sul modo migliore per proteggere il tuo conto.
- Se pensi di essere stato vittima di una truffa avverti immediatamente la tua banca.

Esistono molti modi coi quali i malfattori cercheranno di raggirarti, questi sono i principali.

Phishing – Viene utilizzato un email o un messaggio di testo per ottenere le tue informazioni personali facendo finta che l'email o il messaggio provenga da na fonte affidabile come una banca, un ente caritatevole o il governo. Il messaggio sembra reale e chiede spesso di inserire le tue informazioni personali su siti web fasulli o di cliccare su di un link – ciò consentrà al malfattore l'accesso al tuo computer e alle tue informazioni personali.

Truffe nel fare acquisti online – I truffatori fanno finta di essere veri negozi online, con una sito web fasullo o con pubblicità fasulla in un sito web commerciale genuino. I siti fasulli per gli acquisti online spesso richiedono metodi di pagamento inusuali, come pagamento anticipato tramite vaglia postali, bonifici, trasferimento internazionale di fondi o buoni regalo.

Frodi a danno di investitori – Il truffatore sostiene di essere un agente di borsa o un gestore patrimoniale che offre consulenza finanziaria o sugli investimenti. Ti chiederà di consegnare denaro per un'opportunità d'investimento che può essere reale o fasulla, salvo poi tenersi i soldi.

Frodi per l'accesso remoto – Il truffatore sostiene che c'è qualcosa che non va col tuo computer o con la tua connessione a internet, o che il tuo sistema è stato infettato con malware. Cercherà di convincerti a installare un'applicazione o a consentire l'accesso al tuo computer. Userà ciò per accedere alle tue informazioni personali o domandare una 'tariffa' per risolvere il problema.

Truffe in materia di rapporti interpersonali e amorosi - Il truffatore avvia con te una relazione per estorcere denaro o regali. La relazione si sviluppa gradualmehte e il truffatore ti può chiedere che tu trasferisca beni a suo nome o di diventare beneficiario del tuo testamento. Spesso, ti può chiedere denaro per risolvere un problema di salute, di viaggio o familiare.

LINK UTILI:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/

Nota importante: Questo foglio informativo offre informazioni di natura generale e non intende dare consigli su cui fare affidamento riguardo a qualsiasi argomento particolare. Dovresti contattare la tua banca su come queste informazioni si possono applicare alla tua situazione.