Riepilogo presentazione online

Australian Government

Be Connected
Every Australian online.

Riesci a riconoscere una truffa?

Essere consapevole delle truffe e di come funzionano è uno dei passi importanti per evitarle. Ogni anno gli australiani più anziani perdono milioni di dollari per via delle truffe. Anche se Internet è un posto fantastico da esplorare e per mettersi in contatto con gli altri, non possiamo essere sempre sicuri che le persone siano chi dicono di essere. Una volta che conosci i trucchi di un truffatore, è più probabile che tu sia in grado di individuare una truffa.

Le truffe di phishing

Con le truffe di phishing i truffatori tentano di indurti a credere che chi ti sta contattando è un'organizzazione fidata o una persona che conosci con il fine di farti rilasciare informazioni personali come il numero dei tuoi conti bancari, le tue password e i numeri delle tue carte di credito.

I messaggi di phishing sono pensati per sembrare veri e spesso copiano il formato utilizzato dall'organizzazione che il truffatore fa finta di rappresentare, incluso il marchio e il logo dell'organizzazione. Queste truffe possono assumere molte forme tra cui email, messaggi di testo oppure chiamate telefoniche. Per esempio, potresti ricevere:

- Un messaggio di testo della tua banca che ti chiede di confermare la tua password
- Un'email dal tuo fornitore di servizi Internet che ti chiede di aggiornare i tuoi dettagli
- Un messaggio di testo da un familiare che utilizza un nuovo numero di telefono e che ti dice di aver perso il telefono e che ha bisogno che gli invii urgentemente del denaro
- Una chiamata da un istituto finanziario per avvertirti che ci sono state "attività sospette e non autorizzate sul tuo account", oppure che il tuo account verrà chiuso se non aggiorni i dettagli
- Una notifica di Facebook da parte di una persona che conosci e che ti raccomanda un sito web.

Truffe relative alle imposte e a Medicare

I truffatori si fanno passare per l'Australian Taxation Office (ATO), Medicare ed altre organizzazioni governative per ingannarti e indurti a fare pagamenti e a condividere le tue informazioni personali. Questi truffatori creano siti web falsi e ti invieranno email, messaggi di testo e ti chiameranno facendo finta di far parte di un'organizzazione governativa.

L'ATO non ti manderà mai email o messaggi di testo, né ti chiamerà per farti:

- Condividere le tue informazioni personali come il tuo numero identificativo fiscale, i dettagli della tua carta di credito o del tuo conto bancario
- Pagare una commissione per ricevere il rimborso fiscale o per evitare di essere arrestato per evasione fiscale
- Cliccare su un link per inserire i tuoi dettagli personali
- Scaricare file o installare software.

Se non sei sicuro che la comunicazione sia da parte dell'ATO, chiama la linea diretta ATO Scams al numero 1800 008 540 oppure visita ato.gov.au/scams.

In che modo puoi proteggerti

- Rallenta. Rileggi il messaggio. Chiediti se il messaggio o la chiamata potrebbero essere falsi.
- È un indirizzo email ufficiale o sembra strano?
- A chi è indirizzato? Diffida se si rivolge a "Gentile cliente" invece di usare il tuo nome.
- Contiene errori di battitura o grammaticali? Questo può essere un segno che proviene da un truffatore.
- Non utilizzare i dettagli di contatto forniti nel messaggio: potrebbero essere falsi. Effettua una ricerca su Internet per trovare il numero telefonico dell'organizzazione e il suo sito web ufficiale.
- Non cliccare su nessun link e non aprire nessun allegato in quanto potrebbero scaricare un virus sul tuo dispositivo: premi semplicemente elimina (delete).
- Non fornire dettagli personali come il codice fiscale (tax file number, TFN), la data di nascita, i dettagli del conto bancario o della carta di credito.

Ricorda: i truffatori potrebbero cercare di far leva sui tuoi sentimenti per farti reagire e non darti tempo di pensare attentamente alla situazione. Le loro tattiche potrebbero includere l'utilizzo di minacce o multe, potrebbero dirti che ci sono state delle spese non autorizzate sul tuo conto oppure potrebbero far finta di essere un familiare che ha bisogno di aiuto.

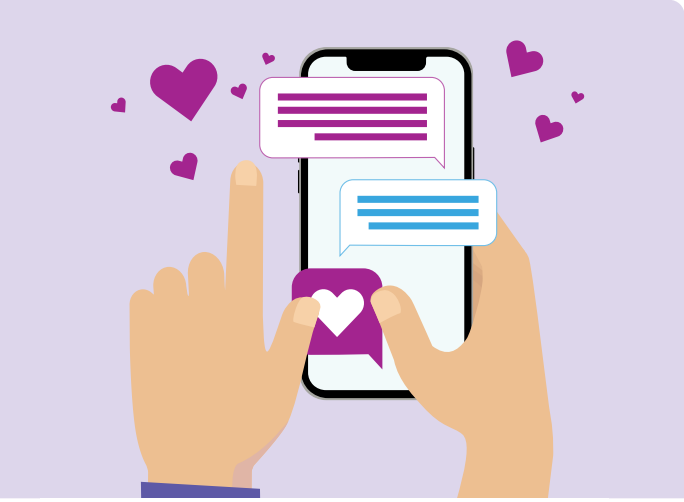
Truffe romantiche e di amicizia

I truffatori si approfittano delle persone che cercano amici o relazioni romantiche, spesso per mezzo di siti web o app di appuntamenti, social media o addirittura giochi online facendo finta di essere potenziali compagni. Il loro scopo è ottenere la tua fiducia al fine di farti inviare denaro, regali, immagini intime o dettagli personali.

Cosa puoi fare per sapere come comportarti e non correre rischi?

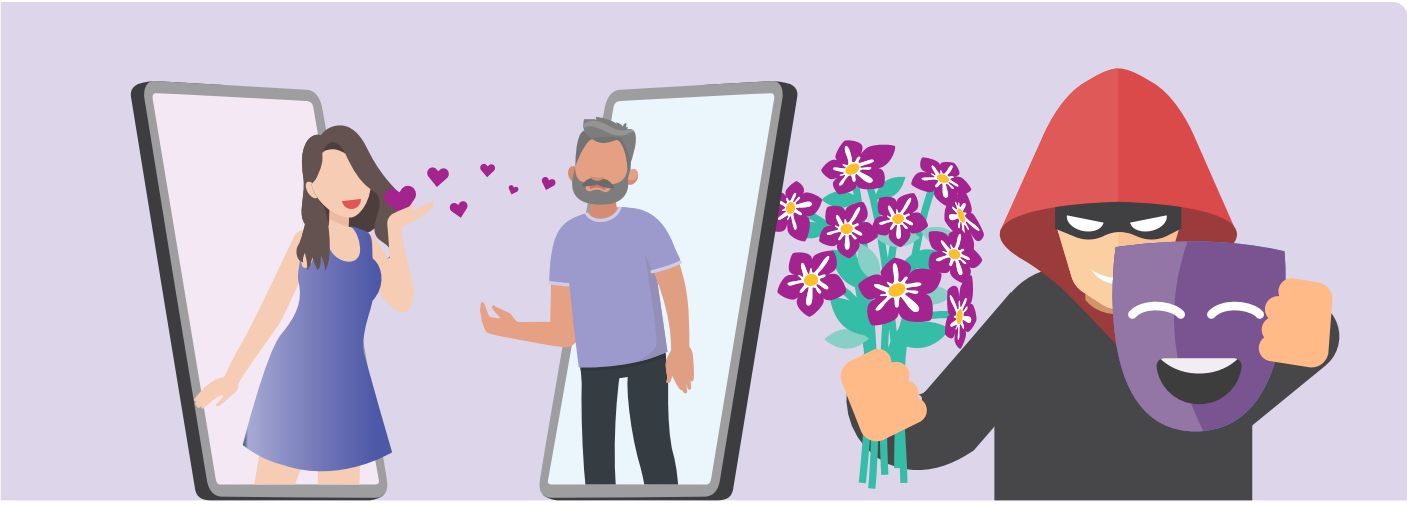
Stai attento a chi:

- Esprime sentimenti profondi nei tuoi confronti molto rapidamente
- Dopo aver ottenuto la tua fiducia (spesso aspettando settimane, mesi o addirittura anni) ti racconta una storia elaborata e ti chiede dei soldi oppure un prestito, regali oppure i dettagli del tuo conto bancario/della tua carta di credito
- Evita di incontrarti di persona e trova scuse per giustificare il fatto che non può spostarsi per incontrarti
- Ha un profilo online che non corrisponde a quello che ti racconta su di sé.



In che modo puoi proteggerti

- Non inviare mai denaro e non dare mai i dettagli della carta di credito, i dettagli dell'account online, oppure copie di documenti personali importanti a qualcuno che non hai incontrato di persona.
- Effettua una ricerca per immagini su Google delle foto della persona per aiutarti a determinare se è veramente chi dice di essere o se le foto sono state prese da qualcun altro su Internet. Vai su images.google.com e fai clic sull'icona della fotocamera.
- Sii sospettoso quando inizia a parlarti di problemi di denaro o ti dice che ha bisogno di soldi per un "emergenza".
- Stai attento a cose come gli errori di ortografia e di grammatica e alle incoerenze nelle storie che racconta.
- Non condividere immagini o video intimi. È risaputo che i truffatori ricattano i loro bersagli utilizzando materiale compromettente.



Truffe di supporto tecnico

Queste truffe di solito iniziano con una chiamata o un'email che sembra provenire da una grande compagnia di telecomunicazioni o informatica, come ad esempio Telstra, NBN o Microsoft nella quale ti viene detto che hai un problema con il computer o con Internet e che l'organizzazione può risolverlo. Richiederanno poi accesso remoto al tuo computer per “trovare qual è il problema” oppure cercheranno di farti comprare un programma inutile o un servizio per sistemare il computer.

In che modo puoi proteggerti

- Se ricevi una chiamata inaspettata in relazione al tuo computer e ti viene richiesto l'accesso remoto, riaggancia.
- Non fornire ad una persona che ti chiama inaspettatamente l’accesso remoto al tuo computer.
- Non condividere informazioni personali come i dettagli del tuo conto bancario o della tua carta di credito.
- Non acquistare software attraverso una chiamata o email indesiderata.
- Ignora i messaggi pop-up che ti dicono di chiamare l'assistenza tecnica.

Consigli preziosi per evitare le truffe

Fermati

- Fermati a riflettere prima di dare del denaro o delle informazioni personali a una persona qualsiasi.
- I truffatori si offriranno di aiutarti o ti chiederanno di verificare chi sei. Fingeranno di far parte di organizzazioni che conosci e di cui ti fidi come ad esempio un'azienda con cui hai contatti, la polizia, il governo oppure un servizio per le truffe.

Pensa

- Chiediti se il messaggio o la chiamata potrebbero essere falsi.
- Non cliccare mai un link in un messaggio e chiedi a un amico o a un familiare fidato cosa farebbero. Contatta le aziende o il governo utilizzando solamente i dettagli di contatto presenti sul loro sito ufficiale o sulla loro app sicura. Se non sei sicuro dì di no, riaggancia oppure elimina.

Proteggi

- Agisci rapidamente se ti sembra che ci sia qualcosa che non va.
- Contatta immediatamente la tua banca se perdi denaro o informazioni personali oppure se noti delle attività insolite sulle tue carte o sui tuoi conti. Chiedi aiuto ad organizzazioni come IDCARE e denuncia il crimine online su ReportCyber. Aiuta gli altri segnalando le truffe su Scamwatch.

Aiuto, sospetto di essere vittima di una truffa

Se pensi di essere vittima di truffa, non ti sentire imbarazzato e non tenerti tutto per te. Ci sono delle cose che puoi fare per risolvere il problema:

- Contatta immediatamente la tua banca o il tuo istituto finanziario per interrompere qualsiasi ulteriore pagamento al truffatore.
- Se sei stato vittima di un crimine informatico e hai perso del denaro online, puoi denunciare il fatto alla polizia per mezzo di ReportCyber oppure visita: cyber.gov.au
- Se sei preoccupato che le tue informazioni personali siano state esposte e utilizzate in modo improprio, contatta il servizio nazionale australiano di assistenza virtuale e per l'identità IDCARE al numero 1300 432 273 oppure visita idcare.org
- Denuncia la truffa ad ACCC attraverso la pagina scamwatch.gov.au/report-a-scam. Ci aiuta ad avvertire le persone sulle truffe correnti, a monitorare gli andamenti e a interrompere le truffe dove possibile.
- Diffondere informazioni ad amici e familiari per proteggerli.

Ricorda: c'è sempre qualcuno che ti può aiutare, sia che si tratti di qualcuno a cyber.gov.au oppure scamwatch.gov.au, o di un amico o un familiare con una preparazione tecnica, o persino di un club informatico di zona

Per tenerti aggiornato sulle ultime truffe da evitare, iscriviti agli avvisi e-mail di Scamwatch.

Scopri con calma Be Connected

Be Connected è un sito web completo con risorse gratuite appositamente progettato per assistere gli australiani più anziani a connettersi online senza correre rischi e a navigare in modo sicuro nel mondo digitale. Il sito è utile anche per le famiglie e le organizzazioni comunitarie che vogliono aiutare i membri più anziani della comunità ad accedere a tutti i vantaggi di Internet.

visita beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Questo programma è stato sviluppato da eSafety nell'ambito dell'iniziativa Be Connected.