Riesci a riconoscere una truffa?

Su Internet, non si può sempre essere sicuri che le persone siano quelle che dicono di essere. Essere consapevole che esistono i truffatori in Internet è uno dei passi più importanti per evitarli. Una volta che sei consapevole dei loro trucchi, dovrebbe essere più facile individuare una truffa quando ne vedi una.

Le truffe di phishing

Le truffe di "phishing" sono la forma più comune di truffa in Internet. Possono sembrare provenienti da un'organizzazione fidata e sono progettate per convincerti con l'inganno a fornire i tuoi dati personali tra cui il conto bancario, il numero di carta di credito, il nome utente e le password.

Possono apparire in molte forme:

- e-mail, messaggi di testo o telefonate impreviste che ti chiedono di confermare, aggiornare o reinserire i tuoi dati personali
- messaggi d'emergenza o di minaccia che ti dicono che sta accadendo qualcosa di insolito con il tuo account o che il tuo account verrà chiuso, e che per questo devi fare clic su un link per sistemare il problema
- email inaspettate che ti chiedono di aprire o scaricare un file ".exe" o ".zip".

Suggerimento: se non sei sicuro di un messaggio che hai ricevuto, ricerca su Internet la compagnia da cui sembra ti sia stato inviato e contattala direttamente.

Rallenta. Rileggi il messaggio.

- Chi è il mittente? È un indirizzo e-mail ufficiale o sembra strano?
- A chi è indirizzata? Diffida se si rivolge a "Gentile cliente" anziché usare il tuo nome.
- Contiene errori di grammatica o ortografia? Questo può essere un segno che proviene da un truffatore.

Cosa non fare:

- non fare clic su nessun collegamento
- non aprire nessun allegato in quanto potrebbe scaricare un virus informatico
- non utilizzare i dettagli di contatto forniti nel messaggio: potrebbero essere falsi.

Truffe relative alle imposte e a Medicare

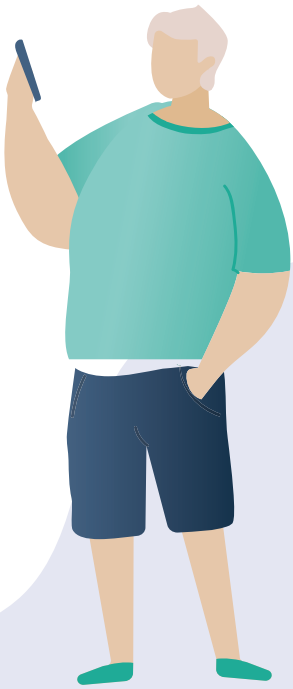
I truffatori si spacciano per l'Australian Taxation Office (Ufficio tributario australiano), per Medicare e per altre organizzazioni governative al fine di ottenere denaro e informazioni personali dalle vittime attraverso siti web falsi, e-mail, messaggi di testo e telefonate.

È importante ricordare che l'Australian Taxation Office (ATO) non farà mai quanto segue:

- inviarti un'e-mail o un messaggio di testo in cui ti vengono richiesti dati personali, ad esempio il TFN, i dettagli della carta di credito o bancari
- chiederti di pagare una commissione per ricevere il rimborso fiscale o per evitare di essere arrestato per evasione fiscale
- inviarti un'e-mail con un collegamento a un servizio online che richiede i tuoi dati personali
- inviarti file scaricabili o dirti di installare software.

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

- Non fare clic su nessun collegamento e non scaricare nessun allegato.
- 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.
- Se non sei sicuro che un messaggio telefonico sia vero, non utilizzare i dettagli di contatto forniti, ma esegui una ricerca su Internet per trovare il numero dell'organizzazione.
- Sappi la tua posizione tributaria: è probabile che ti sia dovuto un rimborso fiscale o che tu debba effettuare un pagamento?
- Accedi al tuo account myGov ufficiale digitando manualmente l'indirizzo invece di fare clic su un collegamento.
- Controlla se l'e-mail che hai ricevuto è dal vero indirizzo dell'ATO che termina con @ato.gov.au
- Anche se sembra che tu sia sul sito web dell'ATO o di myGov, controlla che l'indirizzo finisca in .gov.au (invece di .com.au, .org.au o .net.au per esempio).
- Fai attenzione se vi sono errori di grammatica e di ortografia.
- Diffida dei messaggi non indirizzati direttamente a te.



Truffe romantiche e di incontri

I truffatori stanno creando falsi profili online sui social media o sui siti di incontri per entrare in contatto con le vittime. Il loro obiettivo è quello di guadagnare la tua fiducia prima di chiederti denaro.

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

Stai attento a:

- persone che esprimono sentimenti profondi per te molto rapidamente prima di chiederti dei soldi o un "prestito"
- persone che evitano di incontrarti di persona e trovano scuse per giustificare il fatto che non possono spostarsi per incontrarti
- persone che hanno un profilo online che non corrisponde a quello che ti hanno detto di sé stesse.

Cosa fare:

- controlla se sono davvero quelle persone nelle immagini o se le immagini sono state prese da qualche altra parte in Internet facendo una ricerca di immagini su Google. Vai su images.google.com e fai clic sull'icona della fotocamera
- sii sospettoso quando iniziano a parlarti di problemi di denaro o ti dicono che hanno bisogno di soldi per un'"emergenza".

Cosa non fare:

- non trasferire denaro a qualcuno con cui hai parlato solo telefonicamente o via email
- non inviare informazioni personali come la data di nascita, i dettagli bancari o della carta di credito.

Truffe di supporto tecnico

Queste truffe di solito iniziano con una chiamata o un'e-mail che sembra provenire da una organizzazione di grandi dimensioni nella quale ti viene detto che hai un problema con il computer o con Internet e che l'organizzazione può risolverlo.

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

- Non fornire accesso remoto al tuo computer.
- Non fornirgli informazioni personali come i dettagli del conto bancario o della carta di credito.
- Non acquistare software attraverso una chiamata o e-mail indesiderata.
- Ignora i messaggi pop-up che ti dicono di chiamare l'assistenza tecnica.

Le grandi organizzazioni si aspettano che sia tu a chiamarle quando hai un problema con Internet o con il computer. Non ti chiamano loro.

Aiuto, sospetto di essere vittima di una truffa

Se pensi di essere stato vittima di una truffa, non vergognarti e non tenerlo nascosto. Ci sono delle cose che puoi fare per risolvere il problema:

- contatta la tua banca e interrompi qualsiasi ulteriore pagamento al truffatore
- segnala la truffa all'Australian Competition and Consumer Commission su scamwatch.gov.au: possono aiutarti dandoti ulteriori consigli
- avverti gli altri. Se sai che qualcun altro potrebbe essere stato vittima della truffa, avvertilo.

Se non sei sicuro se un messaggio che hai ricevuto provenga davvero dall'ATO, oppure se sei stato vittima di una truffa relativa alle imposte, chiama la linea informativa **ATO Scam Hotline** al numero **1800 008 540**.

Tieniti aggiornato sulle truffe relative all'ATO visitando ato.gov.au/scams

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 visitando idcare.org

Ricorda:

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

Le truffe hanno lo scopo di approfittarsi della tua bontà, ma Internet può essere un luogo sicuro da esplorare se stai attento a condividere le informazioni personali online, usi il buonsenso quando invii denaro e mantieni la guardia.

Scopri con calma Be Connected

Be Connected è un sito web completo con risorse gratuite appositamente progettato per assistere le persone anziane australiane 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.

beconnected.esafety.gov.au